UNDER THE RADAR: ALTERNATIVE PAYMENT SYSTEMS AND THE NATIONAL SECURITY IMPACTS OF THEIR GROWTH

HYBRID HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT
AND MONETARY POLICY

OF THE

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 20, 2022

Printed for the use of the Committee on Financial Services

Serial No. 117–98

U.S. GOVERNMENT PUBLISHING OFFICE
48–838 PDF WASHINGTON : 2022

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
RITCHIE TORRES, New York
STEPHEN F. LYNCH, Massachusetts
ALMA ADAMS, North Carolina
RASHIDA TLAIB, Michigan
MADELEINE DEAN, Pennsylvania
ALEXANDRIA OCASIO-CORTEZ, New York
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
NIKEMA WILLIAMS, Georgia
JAKE AUCHINCLOSS, Massachusetts

PATRICK MCHENRY, North Carolina, *Ranking Member*
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
ANN WAGNER, Missouri
ANDY BARR, Kentucky
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
WILLIAM TIMMONS, South Carolina
VAN TAYLOR, Texas
PETE SESSIONS, Texas
RALPH NORMAN, South Carolina

CHARLA OUERTATANI, *Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT AND MONETARY POLICY

JIM A. HIMES, Connecticut, *Chairman*

JOSH GOTTHEIMER, New Jersey, *Vice Chair*
MICHAEL SAN NICOLAS, Guam
RITCHIE TORRES, New York
STEPHEN F. LYNCH, Massachusetts
MADELEINE DEAN, Pennsylvania
ALEXANDRIA OCASIO-CORTEZ, New York
JESÚS "CHUY" GARCIA, Illinois
JAKE AUCHINCLOSS, Massachusetts

ANDY BARR, Kentucky, *Ranking Member*
FRENCH HILL, Arkansas
ROGER WILLIAMS, Texas
LEE M. ZELDIN, New York
WARREN DAVIDSON, Ohio
ANTHONY GONZALEZ, Ohio
PETE SESSIONS, Texas

CONTENTS

WITNESSES

TUESDAY, SEPTEMBER 20, 2022

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

UNDER THE RADAR: ALTERNATIVE PAYMENT SYSTEMS AND THE NATIONAL SECURITY IMPACTS OF THEIR GROWTH

Tuesday, September 20, 2022

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY,
INTERNATIONAL DEVELOPMENT
AND MONETARY POLICY,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:07 a.m., in room 2128, Rayburn House Office Building, Hon. Jim A. Himes [chairman of the subcommittee] presiding.

Members present: Representatives Himes, Gottheimer, San Nicolas, Auchincloss; Barr, Hill, Williams of Texas, Davidson, Gonzalez of Ohio, and Sessions.

Ex officio present: Representative Waters.

Also present: Representative Taylor.

Chairman HIMES. The Subcommittee on National Security, International Development and Monetary Policy will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time. Also, without objection, members of the full Financial Services Committee who are not members of this subcommittee are authorized to participate in today's hearing.

I would like to welcome today's witnesses.

We will be doing this as a hybrid hearing, so members will be both physically present as well as piping in on the screen, which is visible to us behind you. It should be visible on either side. We beg your indulgence for any technical issues that may pose, but we do anticipate a good dialogue, both in person and remotely, today.

Today's hearing is entitled, "Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth."

I now recognize myself for 4 minutes to give an opening statement.

Payment systems are the lifeblood of the financial sector. They make sure that banks, businesses, and individuals around the globe can send and receive money without delay and keep the world's economies connected.

The United States and the U.S. dollar in particular occupy a privileged role in the payments sector. As the world's primary reserve currency, our dollar is the most widely used in global trade and cross-border payments. This gives U.S. authorities who are

tasked with oversight immense capabilities to impose financial sanctions and isolate regimes who act against broadly-shared international values.

Earlier this year, we saw how U.S. dollars and the payments system can be leveraged to respond to bad behavior by our adversaries. After Russia invaded the sovereign nation of Ukraine, the United States and our allies acted swiftly to counter Putin's attack by limiting the Russian government's ability to obtain U.S. dollars, and restricting Russian banks from accessing vital international financial messaging systems.

As a result, the Russian economy began to erode, and Putin and his cronies became international pariahs. The world was reminded how U.S. leadership and the U.S. dollar can tighten the screws on governments that violate longstanding norms.

But the strengths and privileges of the dollar are far from uncontested. Around the globe, allies and adversaries alike are taking critical steps to de-dollarize their economies, to develop new methods to facilitate cross-border money transfers, and to control the plumbing of global finance.

In some cases, these alternative payment systems are proactive measures taken by governments to mitigate the expected brunt of economic sanctions and international vilification. In other instances, these systems illustrate the ways that foreign regimes expand their influence in the global payment sector, weaken U.S. competitiveness, and jeopardize the era of dollar dominance.

These systems each pose unique challenges that will require U.S. regulators and the international community to refine our sanctions strategies, closely monitor worldwide financial trends, and keep pace with the rapidly-evolving payment ecosystem to make sure that we are not caught flatfooted.

Our panel this morning will help us understand these challenges and highlight how Congress and the Administration can prepare for alternative payment systems to grow beyond our financial integrity capabilities and compromise our national security. In order for the U.S. to retain its status as a leader in the international payments arena, we must be ready to overcome the obstacles that await us, both in the near term and in the years ahead.

Global leadership in the 21st Century will be determined in part by the oversight and influence of the payment sector. Today I look forward to learning how the United States can best preserve and maintain its status in the global payment system, defend against threats presented by alternative payment systems, and give policymakers and national security officials the right tools to defend our economy against the threats that lie ahead.

With that, I would like to again welcome our witnesses and thank them for helping us to shed light on this important topic.

I now recognize the ranking member of the subcommittee, Mr. Barr, for 5 minutes for an opening statement.

Mr. BARR. Thank you, Mr. Chairman.

And I join the Chair in welcoming our panelists to this hearing.

The rise of alternative payment systems abroad, particularly in China, has deepened Congress' interest in ensuring that our own payments infrastructure remains preeminent. Beijing's development of a digital RMB has also raised the specter of China remov-

ing itself and other countries from a dollar-based financial system, with uncertain effects for our national security.

I look forward to hearing our witnesses delve into these issues today, but let me offer some preliminary thoughts on how we can meet the rise of new payment technologies promoted by U.S. rivals.

First, Congress must foster innovation in our own backyard so that dollar payments are quick, efficient, and secure. This means continually upgrading our payment capabilities, not resting on our laurels.

Already, the Federal Reserve's Fedwire system processes nearly $4 trillion a day, with double-digit annual growth in the volume and value of its transfers. Next year's rollout of FedNow should further facilitate dollar payments for individuals and businesses.

Committee Republicans have been pushing the Fed to prioritize cybersecurity in order to defend these critical functions. We have also underscored the importance of data privacy and cooperation with commercial banks as the Fed considers concepts for a central bank digital currency (CBDC).

If the world is to continue opting for the dollar, we must reject the Chinese model of using financial technology as a tool for government surveillance and control. We cannot and we should not compete with China by becoming more like China.

The private sector is also key. While massive foreign players like Alipay and WeChat loom large, the United States and Europe have launched a diverse array of new payment services, from fintech startups to major technology companies. I am confident that our commitment to competition, free enterprise, and the rule of law will point the way for global standards and payments, not the heavy hand of dictatorships like China.

Second, it is essential for Washington to stop politicizing the institutions that have historically made our financial system the envy of the world. Whether it is the Federal Reserve, the Securities and Exchange Commission, banks, or Silicon Valley, we must resist the call of activists who want to mobilize them against anyone who doesn't share their beliefs. See: ESG.

Just last week, for instance, we held a hearing on de-risking in the Caribbean, where our committee was able to examine how law-abiding businesses in the region are being denied financial services like correspondent banking.

This is a real problem. I only wish our Majority would show a similar concern when their supporters demand that financial institutions pick and choose customers here at home based on environmental and social litmus tests. In the long term, infecting our financial system with political agendas of the day will only make other countries' payment services and currencies more attractive.

Finally, the effectiveness of our sanctions and anti-money laundering regime rests on the dominance of the dollar. As long as this is the case, foreign countries' attempts to evade U.S. law enforcement will be limited. Just ask the Russian Central Bank or cryptocurrency exchanges abroad that have been targeted by the Office of Foreign Assets Control (OFAC).

The dollar is king because its value is market-determined; because we support free capital flows; because our legal system protects investors, rather than preying on them. Dollars give you a

claim to countless high-quality goods and services produced by a $25 trillion economy.

Ultimately, it is economic dynamism and our responsible stewardship of the financial system that will stymie our adversaries' efforts to escape the dollar's reach, as long as we don't stray off course.

China, for its part, is running out of feet to shoot. Its zero-COVID policy is producing urban dystopias throughout that country. Its real estate sector is teetering. And Beijing has shackled itself to Moscow, while the West stands united behind Ukraine. These aren't the moves of a regime that deserves greater sway over the world's financial architecture. And that is a bipartisan sentiment, fortunately.

While China is betting on its financial governance as the wave of the future, global markets have been betting on ours. We must do everything we can to keep it that way.

I look forward to our witnesses' testimony, and I yield back.

Chairman HIMES. I thank the ranking member. I now recognize the Chair of the full Financial Services Committee, the gentlewoman from California, Chairwoman Waters, for 1 minute.

Chairwoman WATERS. Thank you very much, Chairman Himes, for convening this hearing on the current and future national security challenges related to the growth of alternative payment systems. These systems can drive inclusion and offer convenience, but because they are generally outside of the western Federal financial system, they also offer opportunities for sanctions evasion and other financial crimes. Further, they rival U.S. dollar-led trade and payment systems, potentially undermining the strength of the dollar and our ability to leverage tools like economic and trade sanctions.

I look forward to hearing from today's witnesses on what Congress needs to consider regarding this growing concern.

I yield back.

Chairman HIMES. I thank the Chair of the Full Committee, and turn now to our witnesses.

Today, we welcome the testimony of our distinguished witnesses: Emily Jin, a research assistant for the Energy, Economics, and Security Program at the Center for a New American Security; Scott Dueweke, a global fellow for science and technology innovation at the Wilson Center; Dr. Carla Norrlof, a nonresident senior fellow at the Atlantic Council's GeoEconomics Center; Ari Redbord, the head of legal and government affairs at TRM Labs; and Jonathan Levin, the co-founder and chief strategy officer at Chainalysis.

Witnesses are reminded that their oral testimony will be limited to 5 minutes. You should be able to see a timer that will indicate how much time you have left. I would ask that you be mindful of the timer so that we can be respectful of both the other witnesses' and the committee members' time.

And without objection, your written statements will be made a part of the record.

Ms. Jin, you are now recognized for 5 minutes for an oral presentation of your written testimony.

STATEMENT OF EMILY JIN, RESEARCH ASSISTANT FOR THE ENERGY, ECONOMICS, AND SECURITY PROGRAM, CENTER FOR A NEW AMERICAN SECURITY

Ms. JIN. Chairwoman Waters, Ranking Member McHenry, Subcommittee Chairman Himes, Subcommittee Ranking Member Barr, and distinguished members of the subcommittee, thank you for the opportunity to testify before you today and for your interest in the important policy area of payment systems and national security. It is an honor to share the panel with my fellow witnesses.

I study China's alternative payment systems and rails, principally the Cross-Border Interbank Payment System (CIPS), and the digital RMB, or eCNY, in the context of great-power competition between the United States and China.

My testimony addresses China's progress in building out these two alternative payment systems, the implications of growth in these payment systems, and recommends a policy posture to prepare America for a future where alternative payment systems are more prominent than they are today.

First, on CIPS, we should understand what CIPS is and what it is not. It is an RMB clearing and settlement mechanism that facilitates cross-border RMB transactions. It is not China's version of the Society for Worldwide Interbank Financial Telecommunications (SWIFT)—yet—as it does not provide messaging services broadly to global financial institutions.

Second, on the digital RMB, the digital RMB, or the eCNY, is the digital version of the Chinese national currency, the RMB. It is a national payment structure that is mostly domestic and retail which has been implemented across all levels of Chinese society. It, however, increasingly has potential cross-border applications and implications.

At their current stages, these two alternative payment systems are not threats to the mainstream financial system. However, they are growing in technical sophistication and domestic adoption. CIPS use is on an upward trajectory, and digital RMB pilot projects are penetrating through all levels of Chinese society.

Under an ambitious Chinese leadership that envisions more prominent roles for Chinese institutions and international finance, these systems could gain traction internationally and scale up accordingly, with the right geopolitical conditions, over the long run.

In such a scenario, Chinese alternative payment systems and coalitions of alternative payment systems could eventually erode the ability of the United States to use financial sanctions as a deterrent or a punishment in the event of a Taiwan crisis or other geopolitical scenarios.

Moreover, these payment systems could challenge the institutions under the current financial order. The United States, as a leader in the global financial order, needs to respond to this long-term risk today.

The United States cannot control the way other countries are developing their systems. The United States can, however, craft sound policy to influence the march of global payments innovation and maintain U.S. leadership in the international financial system.

Out of my list of recommendations, I will highlight three.

First, the United States Government should support institutions that conduct research on America's and China's financial statecraft. The Department of the Treasury, the Federal Reserve Board of Governors, and the Federal Reserve Banks should designate units of analysts to conduct annual assessments of currency flows in the global payment systems. These analytical units should monitor the use, growth, and connectivity of these alternative payment systems.

Second, Congress should consider mandating the drafting of a long-term strategy document, updated every 2 to 4 years, to signal the direction of U.S. financial statecraft and the United States' thinking for the future of the dollar. This will not only instill confidence in the American private sector that U.S.-dollar preeminence is a priority, but it would also provide clarity to our allies and partners on the United States' financial statecraft posture.

Third, the Treasury Department should develop policy measures to prevent sanctioned entities from taking advantage of alternative payment systems. There should be predetermined policy triggers. If there is proof that Chinese financial institutions cleared and settled transactions with sanctioned individuals or organizations through CIPS, the Treasury's Office of Foreign Assets Control (OFAC) should consider financial sanctions or secondary sanctions on financial institutions that facilitated these transactions. The Department of the Treasury should study the impact of such sanctions prior to levying such tools, given the high likelihood of knock-on effects from such actions.

In summary, I recommended a policy posture that is informed, anticipatory, but not overly alarmist. After asking the question on how alternative payment systems are developing, the United States should focus on how it can maintain leadership in international finance and continue to exert influence in the global financial economic system to serve American national interests.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Jin can be found on page 33 of the appendix.]

Chairman HIMES. Thank you, Ms. Jin.

Mr. Dueweke, you are now recognized for 5 minutes.

STATEMENT OF SCOTT DUEWEKE, GLOBAL FELLOW, SCIENCE AND TECHNOLOGY INNOVATION, THE WILSON CENTER

Mr. DUEWEKE. Thank you.

Esteemed members of the House Financial Services Committee, Chairman Himes, Ranking Member Barr, Chairwoman Waters, and Ranking Member McHenry, I would like to thank the committee for inviting me to testify on this often-ignored area of the modern financial world.

I would like to briefly describe the outlines of the risks presented by the use of virtual currencies to the United States and its allies in the Western world.

Please also refer to my written testimony for greater detail regarding my thoughts on the great advantages of many, but not all, of these systems to the billions of unbanked and underbanked people around the world. It is not all bad.

The scope of virtual currencies extends far beyond Bitcoin and other cryptocurrencies and includes many alternative payment systems you are familiar with, such as PayPal or Western Union, but also included are hundreds more that you might not be familiar with. Some of these, such as Russia's, "dark PayPals," as I call them, including WebMoney and Perfect Money, have often been used by criminals, especially Russian criminals.

QIWI, as I previously testified before the Senate Judiciary Committee, was used to purchase Facebook ads attempting to influence the 2016 U.S. Presidential election. The nexus between adversarial, illiberal regimes and cybercrime cartels acting as their proxies using these systems is clear.

These alternative payment systems are not small, with China's centralized virtual currencies, WeChat Pay and Alipay processing 294.6 trillion yuan, or about $45.6 trillion, in 2020. This dwarfs the $15.8 trillion in all crypto-related transactions that Mastercard's CipherTrace estimated occurred in 2021.

While public blockchain intelligence systems, like Chainalysis, TRM, and CipherTrace, are beginning to do peel-chain analysis, where cryptocurrencies are exchanged for others to obfuscate their origins or usage, they do poorly when assessing where the money goes after conversion into a privacy coin, a centralized virtual currency like Alipay, or other alternative payment systems.

Traditional, follow-the-money approaches often miss the role played by the alternative payments ecosystem—I will call it the, "APE," for short—especially when executed without a generalized understanding of the varied and constantly-morphing set of companies and services that are part of it.

Focusing only on cryptocurrency risks misunderstanding this global thriving ecosystem. Combined, these virtual currencies, mobile payment systems, remittent systems, and stored-value-card systems fuel the shadow economy, as well as enabling very positive changes for the world's unbanked and underbanked. I define this as an ecosystem because they are all connected through hundreds of virtual currency exchanges, converting one alternative payment system for another and another or to and from fiat.

Anonymity or misattribution lives there, where Know Your Customer (KYC) practices are being poorly applied or ignored entirely, especially outside of the West. Financial Open-Source Intelligence (FOSINT), should be developed as a discipline, as well as building tools to understand and monitor this ecosystem as a whole.

The very stability of the global financial ecosystem, at least as we are familiar with it today, is being threatened as this APE has exploded in popularity and viability, becoming woven into the global social fabric. It provides a growing and capable set of interconnected, non-bank financial channels that may or may not ever touch the traditional financial system.

The internet has connected them, just as SWIFT and automated clearing house (ACH) messaging networks provided the original connectivity for banks and other financial institutions to build our current payment system. These traditional bank-centric financial systems are under siege as the ground beneath them shifts amid the awakening of the unbanked and underbanked as well as the burgeoning global middle class.

Frequent use of financial sanctions has contributed to this shift, as Chinese and Russian new payment systems bypass SWIFT and other Western-dominated financial backbones. No longer the domain of fintech startups, nor just limited to cryptocurrencies, nation-states are playing, "the Great Game," on this new terrain.

Increasingly, the high ground of that terrain will be central bank digital currencies. Nine countries have launched central bank digital currencies (CBDCs). Another 15 are in pilot and 16 are in development. The United States is not one of them, although President Biden's recent Executive Order on digital assets is a positive statement of intention to enter that arena.

Currently, the United States is able to monitor and regulate most global payment flows of dollars, but CBDCs and other new payment systems are already limiting our ability to track cross-border money flows. In the long term, the absence of U.S. leadership in standard-setting will have geopolitical consequences, especially if China maintains its first-mover advantage in the development of CBDCs.

If China, alone or with other BRIC countries, is able to combine their non-crypto virtual currencies with a viable CBDC, then soon there will be a real financial and national security problem beyond your ability to regulate. If that day comes—and it could be sooner than most think—the West's ability to dominate the world's financial sphere of soft power will lesson. Without action, our ability to lives in a rules-based financial system will fade with it.

Thank you.

[The prepared statement of Mr. Dueweke can be found on page 32 of the appendix.]

Chairman HIMES. Thank you, Mr. Dueweke.

Dr. Norrlof, you are now recognized for 5 minutes.

STATEMENT OF CARLA NORRLOF, NONRESIDENT SENIOR FELLOW, ECONOMIC STATECRAFT INITIATIVE, GEOECONOMICS CENTER, ATLANTIC COUNCIL

Ms. NORRLOF. Thank you, Chairwoman Waters and Ranking Member McHenry, and also Subcommittee Chairman Himes and Ranking Member Barr, for inviting me to testify on this important topic. I am deeply honored.

My testimony is based on an upcoming report written for the Frankfurt Forum, organized by the Atlantic Council's GeoEconomics Center and Atlantik-Brucke.

Alternative payment systems pose national security risks because they could undercut the dominant role of the dollar in the international currency system. The dollar is by far the most frequently and widely used currency by both governments and private actors. It is used across all currency functions, and it is the only currency that is truly global.

There is no immediate- or even medium-term threat to the dollar's dominance. Even over the long term, it is likely to stay dominant in absolute terms. Other payment systems could, however, threaten the dollar's relative dominance. And we are already seeing a relative decline in the dollar's status.

For at least 2 decades, the international currency system has been strictly unipolar, but after 2017, the system became less

unipolar, and in some years, came very close to becoming a bipolar or multipolar system. Even if relative decline towards other currency majors persists, an end to the dollar's absolute dominance is nowhere in sight. But relative decline could become an issue.

Sanctions are likely motivating some countries to diversify away from the dollar and to devise alternative payment systems to avoid use of the dollar and storing assets in countries where they can be seized.

As a countervailing tendency, however, countries joining U.S. sanctions efforts, as well as countries supporting sanction objectives short of imposing sanctions themselves, continue to have geopolitical incentives to diversify into the currencies by the sanctioning coalition, including dollars. Preliminary analysis of diversification out of Western currencies following the sanctions on Russia in February 2022 suggest very modest diversification out of dollars, some diversification out of pound and yen as well, and diversification into Chinese RMB, other currencies, and euros.

If alternative payment systems expand to involve many countries and private users and cover a wide array of commercial and financial transactions, the dollar will inevitably play a less prominent role than it has in the past. And this is a scenario worth considering.

With the decline in the dollar's importance in the international economy, the economic and geopolitical benefits the United States enjoys as a result of issuing the dominant currency will also decline. An acute weakening of the dollar's global role will jeopardize the United States' ability to influence, stabilize, and enforce international order. The national security ramifications could be quite significant.

Whenever possible, the United States should, therefore, work with allies to gain support for major sanction initiatives, as in the case of the recent sanctions against Russia. To mitigate the growth in alternative payments, the United States should avoid sanctions considered to be unfair or overly harsh. The United States should exhaust softer diplomatic influence attempts before reaching for sanctions, even when maximum campaigns, such as blocking a central bank's reserves, are not being considered.

By signaling a commitment to dialogue and cooperative solutions in the overall use of sanctions, undecided nations are more likely to remain within the familiar, liquid dollar system than to sign up to uncertain, less-liquid alternative payment systems.

Lastly, the United States cannot afford to simultaneously adopt a hard line towards foes and allies. The sharpest decline in the polarity of the international currency system coincides with an uptick in sanctions at a time when President Trump adopted a tough stance against allies, making them insecure about U.S. security commitments.

Thank you very much.

[The prepared statement of Dr. Norrlof can be found on page 67 of the appendix.]

Chairman HIMES. Thank you, Dr. Norrlof.

Mr. Redbord, you are now recognized for 5 minutes.

STATEMENT OF ARI REDBORD, HEAD OF LEGAL AND GOVERNMENT AFFAIRS, TRM LABS

Mr. REDBORD. Thank you.

Thank you, Chairwoman Waters, Ranking Member McHenry, Subcommittee Chairman Himes, Subcommittee Ranking Member Barr, and members of the committee for holding this hearing and inviting me to participate. 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, the blockchain intelligence company.

What is blockchain intelligence? At TRM, we analyze public data from 25 blockchains and from over a million different digital assets. We then combine that publicly-available data with advanced analytics and proprietary threat intelligence to provide unique insights on fraud, financial crime, and national security risks to cryptocurrency businesses, financial institutions, law enforcement, and regulatory agencies worldwide.

I hope that through my written and oral testimony today, the subcommittee can benefit from some of those unique insights.

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

During my time at Treasury, every morning I walked past the Secretary's office, where there was a painting of Alexander Hamilton. 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 opportunity.

Both adversaries and allies alike are exploring alternative payment systems that may circumvent the U.S. financial system, impacting the primacy of the U.S. dollar, the efficacy of U.S. sanctions, and the ability for the U.S. to monitor financial crime.

However, as non-democratic regimes attempt to build alternative payment rails through centralized government brute force, there is an alternative: We can enable the free market to innovate faster on solutions that incorporate democratic principles.

One place this is happening today is with 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 enable consumers to seamlessly send money between companies across the globe. This could spur financial inclusion, lead to more competitive markets, and give consumers lower prices and greater choice.

And, according to TRM's analysis, 99 percent of fiat-backed stablecoin value is tied to the U.S. dollar. Supporting the growth of dollar-backed stablecoins operated by regulated U.S. entities by establishing rules that ensure stability, security, and interoperability can help protect dollar primacy, ensure the efficacy of sanctions, and spread democratic principles across the world.

The native properties of public blockchains—data that is transparent, traceable, public, permanent, private, and programmable—can enable law enforcement and regulators to more readily identify

risks and more effectively and efficiently detect and investigate financial crime.

The nature of public blockchains even facilitates the implementation of effective sanctions. For example, after North Korea's March 2022 hack of the Ronin Bridge, where cybercriminals stole over $600 million in cryptocurrency, OFAC used blockchain intelligence to quickly trace the stolen funds.

OFAC then sanctioned both the blockchain addresses to which the funds moved, and the mixing services that North Korean cybercriminals had utilized to launder over a billion dollars of cryptocurrency. These rapid sanctions designations were possible only because of the transparent nature of public blockchains.

According to TRM analysis, total monthly deposits into one of those mixers, Tornado Cash, decreased by 68 percent in the month after it was sanctioned.

The strength of U.S. sanctions comes not from the primacy of the U.S. dollar alone, but also from the fact that the U.S. is home to innovative companies and people who are transacting in a global economy. The key to effective U.S. sanctions is to ensure that businesses that are leading in the new digital economy remain 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, the U.S. can be home to leaders of this new economy.

As the White House wrote in the framework for digital assets published last week, U.S. companies lead the world in innovation. Digital asset firms are no exception. This should be a clarion call to a race to create and serve businesses in this new economy.

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 is 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 thrive in a growing financial system.

Thank you, and I look forward to answering your questions today.

[The prepared statement of Mr. Redbord can be found on page 88 of the appendix.]

Chairman HIMES. Thank you, Mr. Redbord.

Mr. Levin, you are now recognized for 5 minutes.

STATEMENT OF JONATHAN LEVIN, CO-FOUNDER AND CHIEF STRATEGY OFFICER, CHAINALYSIS INC.

Mr. LEVIN. Thank you.

Chairwoman Waters, Ranking Member McHenry, Chairman Himes, Ranking Member Barr, and distinguished members of the committee, thank you for inviting me here today to testify in front of you.

My name is Jonathan Levin, and I am one of the co-founders of Chainalysis. Chainalysis is the world leader in cryptocurrency investigative and compliance solutions.

Before Chainalysis, 15 years ago, I spent a summer in Shanghai, and at that time the Chinese financial payment system was broken. I couldn't withdraw cash at the same bank when I went on a trip to Beijing. In the past 15 years, however, China has made

enormous progress when it comes to financial innovation and mobile payments.

They are now looking to export their domestic systems internationally through their domestic companies and through their foreign investments in other financial technology firms, and further innovation with a CBDC, as previously mentioned in this witness testimony.

We must have a response.

I have spent the last decade building Chainalysis and sitting on many task forces to actually improve our domestic payment system. All of this has been targeted at our domestic payment system and not at international competition.

Cryptocurrencies actually mark the first innovation that is consistent with U.S. values and poses a real competitive threat to China's financial innovation strategy and their bid to own the financial rails for the 21st Century.

China cannot have a financial payment system that prioritizes strong guarantees over property rights and financial privacy. We must therefore mitigate the national security risks that arise from cryptocurrencies to unlock their strategic potential.

Chainalysis' tools are used by government agencies around the world to investigate the illicit use of cryptocurrencies.

And I want to highlight that the transparency of cryptocurrencies enhances the government's ability to detect, attribute, and ultimately disrupt the illicit use of cryptocurrencies. In many instances, it is actually, in fact, easier to investigate cases involving the illicit use of cryptocurrencies than other traditional means of payment or some of the alternative payment systems that we are talking about.

Furthermore, the percentage of illicit activity in cryptocurrencies is well below the 3- to 5-percent estimates, globally, of money laundering in our financial system.

That being said, because of the transparent nature of cryptocurrencies, there are many stories about illicit activity and funds being identified and actually being recovered.

Recently, in the Ronin Bridge hack that Ari just mentioned, we were proud that our tools could assist the Department of Justice (DOJ) in actually recovering $30 million worth of cryptocurrency stolen by North Korean-linked hackers, which I know is something of great importance and meaning to this committee.

There are many more success stories of how the government has been able to leverage this technology to disrupt illicit activity, starting back at cases that I testified about in front of this committee a few years ago, including the Mt. Gox hack.

In my written testimony, I discuss global trends in cryptocurrency, and provide the background on Chainalysis and how blockchain analysis can be leveraged in investigations. We also delve into the national security threats that are key to this committee and understanding the risks posed by these systems, including its abuse by actors in Iran, North Korea, Russia, and China, and provide recommendations for improving our response to this threat.

In the 20th Century, the United States built the most mature financial system in the world. The guard rails were established to

foster innovation and capital formation where individuals and corporations have clear knowledge of property rights, counterparty risks, and the costs of transacting. The U.S. regulation around commerce on the internet gave rise to the largest corporations in the world.

Cryptocurrencies and stablecoins are already providing these services to consumers and businesses. In fact, we released our global adoption index this week at Chainalysis, highlighting that Vietnam, the Philippines, and Ukraine are among the top adopting countries in the world.

We can ensure that our payment rails are used around the world and that it is built by U.S. companies to serve U.S. principles.

I look forward to answering your questions.

[The prepared statement of Mr. Levin can be found on page 50 of the appendix.

Chairman HIMES. Thank you, Mr. Levin.

I now recognize myself for 5 minutes for questions. I will begin with one question that has a strategic philosophical part and then a request for, kind of, policy recommendations.

My question is this. There is an understandable instinct here to really go hard after the Chinese for their behavior in Hong Kong and Taiwan and Xinjiang and their stealing of our intellectual property, all—the long bill of indictment. And it is an understandable instinct, but it concerns me, because, unlike the situation with Russia, where we do negligible trade and have negligible economic ties, the situation with China could not be more different. They hold $1 trillion of U.S. sovereign debt. They do $2.5 trillion of global trade annually, $600 billion or so of that with the United States.

If we took the approach with China that we have taken with Russia, the devastation to our economy and the global economy would be remarkable. Therefore, I am concerned about proposals to isolate them, to shut them down from the capital markets—some of the proposals around here.

My philosophical question is, strategically, how should we think about countering China in a way that doesn't bring economic apocalypse to us and to the globe?

And then my much more specific policy question is, whatever your answer might be, what specific thing should we be doing with respect to platforms like Alipay and CIPS? Shut them down? Demand accountability?

Again, I will let whomever wants to take the jump-ball, but help me with both that strategic and those specific questions.

Mr. LEVIN. I'm happy to take the jump-ball, although the analogy is a little bit lost on me, but I think I get it.

I think it is a great question. Let me answer the first part first.

I think that when it comes to global competition, there is a big difference between Russia and China. We need to think a lot about what I call asymmetric defense.

The symmetric defense that we have against Russia is the exclusion of them from the financial system. When it comes to China, we have to play a more long-term game. And what I mean by that is that we have a technology race on things like chips, AI, et cetera, where we need to build things that are the most advanced in the world, but that can be easily co-opted and suit the regime in China.

What I think is interesting when it comes to payments is that, actually, our values on financial systems are completely different to that which exists in China. And, therefore, if we can actually foster a place where there are strong property rights, where people's financial privacy is actually guaranteed, with regulation and oversight, we can actually have a financial system for the world that mirrors American values rather than the Chinese.

I think that it is one of these domains where we can actually try and foster a world of financial innovation which actually is diametrically opposed to the values of the Chinese Communist Party.

Chairman HIMES. Mr. Levin, what I am getting from you is that the strategic answer is to build a better mousetrap. Don't worry quite so much about shutting down their product, just build a much better product.

Mr. Dueweke, I saw you raising your hand.

Mr. DUEWEKE. I totally agree with everything Mr. Levin just said.

In addition, emphasizing that the technology, the capabilities to build out on especially blockchain-based solutions—the eCNY is a distributed ledger system. It is not truly the type of blockchain system that we think of, because the Chinese don't want the auditability, the transparency, the ability to provide things like property rights that are not challengeable. What the Chinese want is the ability to collect information on people and to consolidate that information for their own purposes.

So, by basically unchaining the ability of our industry to go ahead and compete, along with much better cybersecurity so that we are not giving up these secrets that we are working on, that is very important.

Second, from all of the other alternative payment systems, we just need to make sure that the Chinese aren't able to expand into areas where they can benefit from having geolocation baked into their systems for all of the users. Certainly, that is something they have tried to do in Europe. We have successfully kept them out of the United States.

And where there are problems with money laundering, threat finance, et cetera, respond to them and to those systems specifically the way—

Chairman HIMES. Let me stop you, Mr. Dueweke.

I have two witnesses now saying, really, the path here is to build out a system consistent with our values, that will be attractive. Is there a dissenting voice or anything added? I only have about 10 seconds, so—

Mr. REDBORD. This is certainly not a dissent, but I would say, look, there is important work to be done on the pressure side as well. The Permanent Subcommittee on Investigations has some great—particularly in the intellectual-property-theft space.

That said, really, sort of, the key to winning here is certainly what we are hearing from Mr. Levin, and Mr. Dueweke, and that is building a better mousetrap.

We are seeing this in the blockchain space today, where China has essentially built blockchain infrastructure that doesn't have the democratic values baked in, that is intended for surveillance and state espionage.

Chairman HIMES. Thank you. I'm sorry. We will hopefully have a chance to continue this conversation, but I need to be a little bit disciplined on time, so that is it for me.

And I now recognize the ranking member for 5 minutes for questions.

Mr. BARR. Mr. Chairman, thank you for convening such an important and interesting and timely hearing.

Let me start with kind of a threshold question. There are two narratives about the advent of digital assets and cryptocurrencies in law enforcement and sanctions evasion.

One is that the pseudonymity of digital assets and cryptocurrencies enable/facilitate criminal activity, enable money laundering, and help ransomware, and it assists sanctions evasion and cyber attacks and the like.

There is another narrative, Mr. Redbord and Mr. Levin, which is that your firms are able to use blockchain technology to assist law enforcement to crack down on these types of illicit activities.

Which narrative is right? Is it a little bit of a combination? Speak to that for us.

Mr. REDBORD. Thank you for the question.

I think you nailed it. The same qualities that make blockchain such a force for good—permissionless, decentralized, cross-border value transfer at the speed of the internet—also make it attractive to illicit actors who want to move funds quickly cross-border.

But the reality is, we have more visibility on financial flows than we have ever had before. When I was a prosecutor, I worked these cases. And now with TRM, we assist law enforcement in investigating fraud and financial crime. And they can trace the flow of funds in ways that you never could with bulk cash smuggling and networks of hawalas and shell companies. And I think the reality is, we are seeing that play out.

For example, there was a recent arrest in a case involving a 2016 hack of the cryptocurrency exchange Bitfinex. But because of the nature of blockchains—this immutable, public ledger that is forever—law enforcement was able to go back and use tools to trace and track the flow of funds in ways you never would be able to in the traditional financial system.

There are certainly ways to sort of move funds in crypto, but there is also more visibility on those financial flows than ever before.

Mr. BARR. Mr. Levin?

Mr. LEVIN. Yes. Thank you, sir, for the question.

I think the one thing I would say is that, to make the second narrative work, we have to change our mindset. We have never had a financial system that is as open as cryptocurrencies and presents the types of opportunities to monitor for illicit activity. And it has to start with a change in mindset for our Executive Branch of how they can actually proactively go after the types of threats that exist.

And what we have demonstrated over the last 8 years is that it is definitely possible, with this technology, to go after criminals and to find them and to take sanctions actions and seizures and really hold people to account.

But actually, as this system proliferates, we need to get proactive with our type of monitoring of the types of threats that exist. And we need to charge our Executive Branch with, how do you do that proactively in an age where this information is out there online, and how do you take a technology-first approach to dealing with these problems in a way that modernizes the type of approach to financial intelligence that we have seen in the past?

Mr. BARR. Let me shift gears to central bank digital currency for a minute. What is the better approach to preserving and protecting and maintaining the dollar's dominance? Is it a Fed-issued digital currency, a central bank digital currency in the United States to compete with the digital RMB? Or is it a regulatory framework for fiat-backed stablecoins to preserve the utilization of the dollar as the world's currency, harnessing private-sector innovation to advance a U.S.-centric version of frictionless, cross-border, secure use of digital currency backed by the dollar?

Which is the better approach, and why?

Mr. REDBORD. I will take a quick crack at it.

I think what is interesting about the question, and certainly, what we hear from the Executive Branch is that there is continued work in the CBDC space. Even as late as last week, we heard from the White House in a very detailed technological discussion that they are still working on a CBDC. And the jury is really still out on whether that will happen at all.

But the reality is that stablecoins are proliferating today globally. And as I said in my statement, 99 percent of those that are backed by fiat currencies are backed by the U.S. dollar, which gives us an incredible opportunity to export our values and our principles abroad through private technology of that kind.

And I think this is a really extraordinary moment, when we see that level of commerce happening in U.S. dollars in the digital space, that this is really a moment to really provide legislative legal clarity to that space today as we still work on figuring out whether or not a CBDC makes sense.

Mr. BARR. My time has expired, but I think it speaks to competing with China, not by becoming more like China, but by doing this the American way.

Mr. REDBORD. Well said.

Chairman HIMES. The gentleman's time has expired.

The Chair of the Full Committee, Chairwoman Waters, is now recognized for 5 minutes.

Chairwoman WATERS. Thank you so very much.

I am so pleased with this hearing and the witnesses that are here testifying today, because we have gained substantial information already, and the questions that are being raised by our members here will help us in so many ways as we move forward.

As you know, we are focused on stablecoins right now, and we are developing legislation because of the volatility, because of the fact that we discovered that the representation for assets that were being held by some of these companies was really not real. It was a lot less than what they said.

And so I really want to know, for Mr. Redbord, with what Mr. Dueweke has described, can you please address the need for the

U.S. to develop a legal and regulatory framework to deal with stablecoins, the market for which is already over $152 billion?

Can we afford to do nothing or delay further Federal action, especially on ensuring that anti-money laundering and sanctions protections are included in this alternative payment method's growth?

Mr. REDBORD. Chairwoman Waters, thank you for the question.

On the one hand, it is critical to ensure that regulation in an emerging space like this is done right. You want to ensure the open process that you have been engaging in and the opportunities for stakeholders to engage.

But, on the other hand, the time is now. In the wake of the collapse of Terra, an algorithmic stablecoin, we have seen policymakers and regulators globally move to provide frameworks for stablecoins. We have seen safety nets through regulation. And it is really a moment to assert U.S. leadership by establishing rules that ensure the stability, security, and interoperability of regulated stablecoins.

In any discussion, it is critical to point out that Terra was very, very different from what we are talking about today, these U.S.-backed stablecoins that will allow us to transact globally in U.S. dollars or U.S.-backed stablecoins.

But as we continue to study the CBDC, the time really is now to act to provide clear regulatory guidance or clear legislative guidance to stablecoin issuers, particularly in this U.S.-backed space, to really give us the opportunity to lead here. The time is really now in this space.

Chairwoman WATERS. Thank you very much.

And since you talked about blockchain quite a bit in responding, I think, to one of our members, what significant role can blockchain play in the identification of alternative payment systems that may not be in the best interests of the U.S. or internationally?

Mr. REDBORD. Absolutely. I think, as we discussed a little bit earlier, blockchains allow for unprecedented visibility on financial flows. And it allows us to identify not just illicit finance and bad actors but also instances that affect market integrity.

And what blockchains really allow, with that permanent, immutable, public ledger, is it allows us to track trends in ways we never could before. Even in preparing for this hearing, we have a blockchain intelligence team at TRM, and they continuously provided updates to me on key insights on data. And this would be impossible without the extraordinary power of open blockchains. We have more insights on financial flows, not just financial crime, than we ever had before.

And we just need to ensure, as we are building blockchain frameworks, just like they are building blockchain frameworks in China, that we are baking U.S. principles and democratic principles into that process.

Chairwoman WATERS. I want to thank you all for your testimony today.

This is so important. As I have described, our first major legislation is dealing with stablecoins. And we know a lot about what has happened with stablecoins up to this point. But we are moving, as you know, to consider where we are going to stand with a CBDC. And so, everything that we could understand and learn about how

to deal with alternative payments, I think is going to be very important.

And while I share our Subcommittee Chair's concerns about China, you must know that many of us are looking very closely at China for everything and trying to make sure that their cooperation with Russia or North Korea is not such that they are gaining ground on us in any aspect of our economy and our democracy.

Thank you so very much for being here today.

Chairman HIMES. The gentlelady's time has expired.

The gentleman from Texas, Mr. Sessions, is recognized for 5 minutes.

Mr. SESSIONS. Mr. Chairman, thank you very much. And my thanks to you and the Chair of the Full Committee, Chairwoman Waters, for providing an insightful and timely opportunity to hear from our witnesses.

And let me congratulate each of you. I think you have given us not only good insight but fair warning of what lies ahead.

I want to go back to—because I think my thinking is a lot like our ranking member, the gentleman from Kentucky, Mr. Barr. And I have changed four or five times in my thinking since then as each of you have spoken.

I only have a few minutes, but let me say this. I have a question, and that question revolves around, if the United States, as we migrate to this stablecoin and we finish the legislation that the gentlewoman has and we move forward—two questions: Number one, can we see, other than knowing what China is after—that they are after more personal information on people, which, here in the United States, we don't want to do that, personal information and data that could be used to control anybody; and, second, about the excessive amount of money that was stolen by gangs as we provided our COVID relief and other things, that goes into the billions of dollars.

How stable and secure are these processes? And do you have any feedback on that?

I guess I would ask, Mr. Levin, if you have an idea, Mr. Redbord, or Mr. Dueweke, because, in particular, I think I focused on specific areas that you have addressed. So if you would take the remaining 3 minutes and 10 secs, perhaps a minute each—

Mr. DUEWEKE. Certainly.

Mr. SESSIONS. —and provide me some context.

Mr. DUEWEKE. And it is a great question because it gets to—especially for the COVID relief, it gets to the very porous natures of a lot of these processes, where you don't have good control.

And the underlying technology of cryptocurrency, including Bitcoin, is, of course, the blockchain. And people often conflate blockchain with strictly financial applications, but, in fact, I have done a lot of work with the healthcare industry, where the blockchain was being used, at least in pilot form, to share identity and to avoid the leaking of personally identifiable information.

It certainly would lend itself well to a process where you are trying to get money out there but you need to understand who it is going to. Now, it is not something you are going to be able to set up immediately in a crisis, but if you have such a system prepared, certainly blockchain would help do that.

Second, as far as stablecoins in general, I think what people are sometimes missing when they focus on it—I agree that it is a way to focus innovation, focus the American way, to building new systems like that. But don't forget that it is part of an ecosystem, and don't forget that it is fungible. And without having controls on that from stem to stern, you are going to lose control quite often.

And even with the stablecoins that are out there today, you oftentimes will see it be converted out of that stablecoin and into something else that isn't trackable—it might be a privacy coin; it might be one of these centralized virtual currencies based in Russia—and then come back in, and you are not going to be able to track that.

Better Know Your Customer (KYC) requirements, I think, are part of this too. We do this first layer of KYC pretty well for who is going to be your customer. Who they are dealing with does not go as well. And, in fact, there are person-to-person exchanges even in the United States where there are publicly-posted requests to buy or sell cryptocurrency and they say that they don't need to have identity of that person.

So, even meeting the requirements of the current regulations and laws as they exist, if they are still allowed to facilitate that type of kind of semi-anonymous transfers at a premium, it is kind of like having the 21-year-old kid next door stand outside of a Kwik-E-Mart and be able to buy legally, and then there will be a line of kids there getting it from him.

It is just not making sense. We have to do better at KYC.

Mr. SESSIONS. Thank you very much.

Mr. Chairman, one last word. I would like to bring down my information to you and have you engage me. I know we have run out of time.

Mr. Chairman, thank you very much. Most interesting, well worth my time.

And the gentlewoman from California, thank you very much.

I yield back.

Chairman HIMES. The gentleman's time has expired.

The gentleman from Guam, Mr. San Nicolas, who is coming to us remotely, is recognized for 5 minutes.

Mr. SAN NICOLAS. Thank you so much, Mr. Chairman. And I would like to echo the sentiments of my bipartisan colleagues. I think this is the second subcommittee hearing we are having that I think has a lot of bipartisan interest.

And Chairwoman Waters, thank you so much for your leadership in helping us to come together on very key issues that are affecting the globe.

I wanted to first just make sure we have it clear on the record, if we can just get a quick, "yes" or "no" across-the-board from the witnesses, but what I am hearing is that every single person on this panel agrees that the United States needs to, in some form or another, whether it is a CBDC or a stablecoin, we need some form of digital currency.

Is that a, "yes," across the panel?

Chairman HIMES. I think he is asking for a, "yes" or "no," from all of the witnesses, so we will start with Ms. Jin and just move to the right.

Ms. JIN. Yes.
Mr. DUEWEKE. Yes.
Ms. NORRLOF. Yes, for CBDC.
Mr. REDBORD. Yes.
Mr. LEVIN. Yes.
Mr. SAN NICOLAS. Thank you.

And, actually, Dr. Norrlof, I would like to direct my next question to you, because—and this is kind of tied into, I think, where Mr. Barr was going earlier, about the difference between CBDCs and stablecoins.

We have the Federal Reserve, and they are responsible for monetary supply and a various host of other responsibilities in the financial system. We also have the U.S. Treasury, and one of their primary responsibilities is the production of coin and currency.

As we navigate going forward what we see as a unanimous need for us to adopt some form of digital currency, where should the leadership really come from? Should the leadership come from the Federal Reserve, or should it come from U.S. Treasury that has a responsibility to produce coin and currency?

Dr. Norrlof?

Ms. NORRLOF. I think that the leadership should come from the Federal Reserve.

I also want to say that, for the CBDC, I think that progress in this area is especially important because that is really where China can make a difference to undercut the dominance of the dollar. If the Chinese CBDC goes forward, we will see a very strong push towards a convertible renminbi, which will put the Chinese currency—really make it much more attractive for international investors.

I would also like to highlight that, for the CBDC, it is not just a China issue; it is a general issue. According to the Atlantic Council's research, there are about 104 countries that are currently exploring CBDCs. And I think that there are real opportunities for the Federal Reserve to assume leadership in this critical area.

Mr. SAN NICOLAS. Thank you.

Mr. Chairman, I just wanted to, I guess, pose the question across-the-board, because I am still trying to come to grips with the idea that what has historically been a Treasury responsibility on the production of coin and currency will now potentially become also a Federal Reserve power, if they are authorized to do so on the digital currency sphere.

And so, I would like to also pose it to the remaining panelists: Is there a consensus that there is a belief that the Federal Reserve should be the one taking the lead on the digitization of U.S. currency, or should it be the Treasury?

I guess we can go from right to left.

Chairman HIMES. Mr. Levin, that would be you. I guess we are going the other way this time.

Mr. LEVIN. Oh, okay. Thank you, sir.

I think that the question of oversight here is primarily about technology.

And I would say that one clarification that I would like to sort of put forward is that, actually, we already have a lot of digital dol-

lars in existence. In fact, a lot of our payment system is digital. We are not, sort of, sitting here with dollar bills.

The Federal Reserve is primarily responsible for the technology that supports how we clear and settle those dollars. And so, it does make sense that as a pure technology play, we think about what the future of that technology stack looks like, and that would come under the Federal Reserve.

And there is some significant work in making sure that all of the institutions that are actually transacting in dollars and have access to that system, actually can have buy-in and weigh-in on the cybersecurity concerns and the AML concerns.

Mr. REDBORD. I agree with Mr. Levin in that it really depends on the technology itself.

If we are talking purely about a CBDC, a central-bank-issued digital dollar, then certainly, obviously, the Federal Reserve is—that is the function that the Federal Reserve has always taken when it comes to our currency.

But when we are talking about U.S.-backed stablecoins globally for payments, that could very well be something that is regulated or the oversight comes from the Treasury Department, just like other sorts of technology, whether we are talking about securities or commodities, could be handled by other regulators.

I think, today, it really depends on the technology.

But, to the first question, the U.S. doubling down on the need for a digital asset that holds our values and exports those values, whether it is a stablecoin or a CBDC, I think is certainly important.

Chairman HIMES. The gentleman's time has expired.

Mr. SAN NICOLAS. Thank you.

Chairman HIMES. The gentleman from Texas, Mr. Williams, is now recognized for 5 minutes.

Mr. WILLIAMS OF TEXAS. Thank you, Mr. Chairman. And thank you for calling this hearing today.

Being from Texas, when I hear about payment systems funding illegal activities, my mind—you know where it goes. It goes to the southern border. This year alone, we have seen the numbers—expecting to see over 2 million people illegally come into this country. It is pretty unbelievable. And this massive influx of people has created a booming industry for drug cartels and human-trafficking organizations.

And it is amazing how much these criminal enterprises have grown over the last few years. Just in 2018, there was an estimated $500 million in illicit revenues along the border. This year, that number has grown to $13 billion.

And I have been to the border. I have been going to the border for many, many years and have witnessed firsthand how chaotic the situation is for the brave men and women on the Border Patrol. We need to pray for them every single day.

The Biden Administration needs to stop turning a blind eye to the disaster—President Biden and Vice President Harris have not even been down there—and get serious about ending this national problem that we have.

When I talk with Border Patrol agents, they say traditionally cash is king for these criminal organizations. However, with the

advent of cryptocurrencies, there is some concern that the ease of cross-border payments has helped fuel this rise in revenue.

Mr. Levin, can you describe the scale that cash is used for illegal activities compared to cryptocurrencies? And, additionally, can you give us a recommendation on how we can better implement technology to track the illicit money flows?

Mr. LEVIN. Thank you, sir, for the question. And it is a very important issue.

The feature of cryptocurrencies is that it does work seamlessly across borders anywhere in the world instantaneously, the same way as the internet. And people think that represents real problems when it comes to the issues that you are talking about.

However, I would say that, in networks, in my experience, where it comes down to drug trafficking, human trafficking, and criminal activity, there are very established means of moving money, and those networks tend to rely heavily on existing financial networks of money laundering, which are very cash-dependent still today.

When it comes to being able to track this more proactively, it is actually possible to look at the flow of funds that go between borders when it comes to cryptocurrencies.

That is what Chainalysis does and it provides that type of intelligence to the agencies that are responsible for tracking down the illicit use of cryptocurrencies—drug trafficking and human trafficking—that can be tied back to specific instances.

And, indeed, I have been sort of familiar with several investigations where cryptocurrencies have actually led to the discovery of these types of networks and the arrests of the people who are perpetrating these crimes.

Mr. WILLIAMS OF TEXAS. Thank you for that.

We have seen a news report for several months that the Biden Administration is trying to revive some form of the Iran nuclear deal. And, unfortunately, the President has been keeping Congress in the dark about how these negotiations are progressing, which is extremely bothering to me and a lot of others, considering this country is still a state sponsor of terrorism.

Just this week, the OFAC took actions against 10 Iranian individuals and multiple businesses for their role in various ransomware attacks.

Again, Mr. Levin, can you describe the methods that Iran is using to commit these cybercrimes?

Mr. LEVIN. Thank you, sir. And it is a very important and timely issue.

According to OFAC, the Islamic Revolutionary Guard Corps (IRGC)-affiliated group is perpetrating cybercrime attacks using known vulnerabilities and gaining unauthorized computer access to devices to extort victims in order to unlock those computers.

What is then possible, due to the transparent nature of cryptocurrency, is that OFAC can, with their partners in other law enforcement agencies, actually track and trace those funds and manage to actually list some of the addresses that were being used to extort their victims, which definitely puts a dent in the financial motivations, if there were some, to perpetrate those attacks.

And what I have seen historically is that we are actually able to track down some of the networks that enable the ransomware and

cybercrime actors within Iran that are causing a disruption to our healthcare system, our education system, and targeting U.S. businesses, and, with the right tools, those agencies can go after them and prevent from financially benefiting.

Chairman HIMES. The gentleman yields back.

The gentleman from Massachusetts, Mr. Auchincloss, who is also the Vice Chair of the Full Committee, is recognized for 5 minutes.

Mr. AUCHINCLOSS. Thank you, Mr. Chairman.

Ms. Jin, my question is for you, to begin with, on China's digital currency.

In January, you published research entitled, "China's Digital Currency: Adding Financial Data to Digital Authoritarianism." The article states that, "The Chinese government hopes to leverage Digital Currency/Electronic Payment, or DCEP, for the Chinese Communist Party's (CCP's) domestic political agenda." This furthers the belief that the CCP's digital currency will have to be taken up at the expense of privacy and individual freedoms.

I want to add my voice to what we have heard from the Republican side of the aisle, that, to contest China's uptake of a CBDC, we do not need to respond with our own CBDC but, rather, with a regulated, competitive marketplace of stablecoins and to let American entrepreneurialism and competition surface the best.

I welcome your input on that, both how the United States might create that ecosystem and also how it might help us compete with the Chinese digital yuan.

Ms. JIN. Thank you so much for your question. To answer it, I might offer a heuristic that I use when I think about the Chinese system and the American system, which is this concept of legibility.

"Legibility" is kind of an old political science term that talks about using simplistic metrics to understand the populace or the citizenry that you are serving. So, it is coming from the perspective of a state.

And we can clearly see in the way that China runs its eCNY or DCEP—it has many names—that the idea is to have an enhanced sense of state-run digital legibility. The idea is to collect as much data as it can on the citizenry. And the data might over time have predictive property as well, depending on the advanced nature of the PBOC's Big Data analytic skill set.

But this has proven to be a very useful way for me, personally, to think about how the United States' and China's systems are different.

On the other side of digital legibility is this respect for digital financial privacy, which is, I would say, the crux of how the U.S. innovation system works, how the U.S. financial technology innovation systems and economic actors work together.

I personally envision, and just according to my research, that the United States' innovation system will be a lot more productive if the regulations, first of all, are clear, but, second, the government is not cracking down or limiting certain innovative actors in essentially doing their jobs or conducting their businesses.

Mr. AUCHINCLOSS. To jump in there—

Ms. JIN. Yes.

Mr. AUCHINCLOSS. And we are making progress on bipartisan stablecoin legislation, which is encouraging.

Do you think it is necessary, just to really burrow down into this point, for there to be a U.S. CBDC for us to outcompete what the Chinese Communist Party is trying to do by creating an alternative financial payment system and digital currency?

Ms. JIN. I don't think it is a necessary condition. However, I do think there is a lot of effort inside the U.S. Government from many different branches considering the possibility for—

Mr. AUCHINCLOSS. So R&D, fine, could help us set the table and enforce international norms, but not actually the production?

Ms. JIN. Not actually the production. But one—

Mr. AUCHINCLOSS. Does anybody on this panel want to disagree with that?

Ms. NORRLOF. I have a point to this.

I think that a lot of the focus here is on digital currencies, and I think that it is important, but I also think that the United States today is not really competing with China. China is trying to catch up, and they are using various methods in order to catch up.

So, the United States does not have to have a central bank digital currency at this point. It could become more interesting at some future point in time. For the Chinese, however, it is quite crucial to have a central bank digital currency in order to get anywhere close to where the United States is today.

Mr. AUCHINCLOSS. Yes, because, Dr. Norrlof, you have written about this, I know, in The Washington Post, about dollar dominance and the Chinese trying to catch up. And you are saying now that we don't need a CBDC to persist dollar dominance?

Ms. NORRLOF. If we are looking at the role of the dollar in the international system, China is nowhere near the United States.

Mr. AUCHINCLOSS. Yes.

Ms. NORRLOF. China is trying to find inroads and various avenues in order to compete with the United States, but it is coming from a very, very low floor.

Mr. AUCHINCLOSS. And could a well-regulated stablecoin marketplace in the United States help us box the CCP out from trying to contest us?

Ms. NORRLOF. I am not sure that it is necessary. I think that it would be, actually, more productive to think about alternative payment systems more broadly. What are other countries doing in order to bypass the dollar? Are they trying to use other currencies, notably the Chinese currency but also, I don't know, like, the Indian rupee—

Mr. AUCHINCLOSS. I need to unfortunately interject—

Ms. NORRLOF. Okay.

Mr. AUCHINCLOSS. —because I am out of time.

And I will yield back to the Chair.

Chairman HIMES. The gentleman's time has expired.

The gentleman from Arkansas, Mr. Hill, is now recognized for 5 minutes.

Mr. HILL. Thank you, Chairman Himes.

Thank you to the panel for sharing your views with the committee today.

And thank you, Chairwoman Waters, for convening this hearing.

And let me say that, first, Chairman Himes and I have a bill, the 21st Century Dollar Act, which essentially asks the Treasury

to do a study that outlines exactly this debate, which is: What are the conditions present that we have to do in this country to make sure the dollar remains the reserve currency of the world and is an effective medium of exchange across the world? And that is important, because right now it is a major advantage to have things denominated in dollars, and we want to maintain that. And part of that would be looking at what role tokenization of the dollar might play.

But, Dr. Norrlof, is the Chinese RMB extremely exchangeable?

Ms. NORRLOF. No. It—

Mr. HILL. No, I am not asking you—just, is it, yes—

Ms. NORRLOF. No.

Mr. HILL. No.

Do they have the rule of law in China, where you would want to be in a Chinese court adjudicating a claim? Would that be—

Ms. NORRLOF. No.

Mr. HILL. —your perfect place?

Ms. NORRLOF. No.

Mr. HILL. No.

And so, no rule of law, no freely exchangeable. The Chinese RMB is not a competing currency, unless we make it one by increasing its basket in the SDR basket at the IMF or doing anything that diminishes the power of the United States to have that valuable dollar.

And I would say that running huge budget deficits and racking up debt and spending money like drunken sailors puts the dollar far more at risk than this debate about digital currency.

But I urge our bill to be marked up and passed into law so that we can have a definitive all-of-government review of how we maintain a 21st-Century, competitive U.S. dollar.

Let me turn to the actual subject of the hearing, if I could, and talk about sanctions-related issues and alternative payment systems. And, again, let me commend the Majority for the hearing.

Since 2014, Russia has attempted to diversify away from the dollar. We have seen that. They have bought the euro, they have bought the yen, they have bought the RMB in their central bank. They have fewer dollars.

When we cut them off in 2014, they decided they would start their own domestic credit card company, be less dependent on Visa/Mastercard. How has Visa and Mastercard's suspension of services in Russia affected domestic issuance and acceptance of Mir cards?

Who wants to answer that?

Yes, sir?

Mr. DUEWEKE. I don't have the exact numbers, but Mir is still a shadow of what Visa and Mastercard had in the country.

And what is interesting, post-2014, post-Crimea, is the way they diversified. In fact, in 2014, I was at The Hague on behalf of the DEA, talking on this topic actually, and the FSB was there. They still had two parts: anti-child-sex-rings, et cetera—they were still working with us on that—and anti-drug. And they talked about how, at that time, the Russian WebMoney system, which is now in over 80 countries, was the, "primary drug money movement mechanism globally for Russian organized crime." Within a year, it had become their PayPal.

Mr. HILL. Yes.

Mr. DUEWEKE. And now, we have Yandex Money and various others, like QIWI, that are found around the world. These alternative payment systems have also then become banks. There is QIWI Bank—

Mr. HILL. Let we interrupt you there. Has China complied with the secondary sanctions, in your view, to prevent UnionPay from being a global interchange for those Mir cards, to replace the interchange that they were getting internationally from Visa, Mastercard, and American Express?

Mr. DUEWEKE. Judging by the Russians who are going into Finland to use their UnionPay cards at ATMs, it doesn't necessarily appear so.

Mr. HILL. So, that is an area that we should talk to Treasury about vis-a-vis secondary sanctions and from a compliance point of view?

Mr. DUEWEKE. Correct.

And I still think it speaks to what the last two speakers have described, which is that China, Russia, the BRIC countries, need that, one of them, to have a big system, much more than we need to have a CBDC. Right? They need a way to do trade amongst themselves.

They have these messaging systems that they can use, the big alternative payment systems. My goodness, Alipay and WePay are just huge—much bigger than all of the crypto times four.

Mr. HILL. Right.

Mr. DUEWEKE. Right? Those systems exist in secure messaging. Using all of those, if you went then and converted it or combined a CBDC, the eCNY, with the mobile payment systems and all of the platforms on phones that people have, you would have a very robust system—

Mr. HILL. Thank you.

Mr. DUEWEKE. —pretty quickly.

Mr. HILL. Thank you. I appreciate it. If you have more, please respond in writing.

And I think this really speaks, Mr. Chairman, to why secondary sanctions and the use of FinCEN is important, because it links all of this together in enforcing our sanctions.

I yield back.

Chairman HIMES. The gentleman's time has expired.

The gentleman from Ohio, Mr. Davidson, is recognized for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman.

And I thank the witnesses for your work in this space.

Chairwoman Waters, thank you for hosting this hearing and paying a lot of attention to this space. I think the future of money is perhaps the most important policy debate going on in Western civilization.

Dr. Norrlof, as you highlight, there are over 100 countries around the world studying central bank digital currencies. My concern is that, of the countries studying it, I am not aware of a single country that is studying a true distributed ledger system that facilitates permissionless, peer-to-peer transactions.

It seems like everyone is tripping over themselves to find a way to develop a tool that is the same creepy surveillance-state system that China is developing, a centrally-managed, centrally-controlled, central bank digital currency that creates a monopoly on money, essentially to turn it into a tool for coercion and control more than what money is supposed to be, which is a store of value and an efficient means of exchange.

This is a corruption of the whole concept of money. And that is why I think that the future of money is so important to Western civilization. If we see money turned into this, the principles and values that have built Western civilization are truly threatened. It might not be this government, but some government will eventually use that power the wrong way. And for people who doubt that, just imagine whomever your political rival is having control of the system of money.

I have been a little concerned as I watch the debate as to the role for Treasury versus the Federal Reserve. It was a good question by Mr. San Nicolas. And I would just point out that, looking at our money, the Secretary of the Treasury's signature is on it, not the Chairman of the Federal Reserve. Looking at our money, it says, "This note is legal tender for all debts, public and private." And cash is actually the only current, truly permissionless, peer-to-peer transaction system. There are a lot of digital systems that are working to rival that.

And I would just ask quickly, so we can continue the conversation, maybe starting from right to left, Mr. Levin, do permissionless, peer-to-peer transactions pose a threat to the financial system?

Mr. LEVIN. Thank you, sir, for the important question.

I think that the permissionless, peer-to-peer transfer is part of the way that the economy works. And we have to find ways where our payment system actually reflects the type of innovation and industrial revolution that we have.

Mr. DAVIDSON. Yes. That is a recognition of fact. Does it pose a risk?

Mr. Redbord?

Mr. REDBORD. I think that it is a major part of the financial system moving forward—permissionless blockchains, peer-to-peer transactions. And we can now enable that with technology.

And I do think, at the end of the day, the choice of what the reserve currency is, is not going to be governments; it is going to be entrepreneurs and people who are transacting in that world. And they are always going to choose the freedom to transact without surveillance and potential state espionage. I believe that, ultimately, entrepreneurs will make the choice for a more permissionless system, and the technology will allow for that.

Mr. DAVIDSON. Yes. Thanks for recognizing that. I think it is an important observation.

And I think governments are trying to cling to the power, fundamentally, which decreases trust. And I think Mr. Hill highlighted why no one is going to adopt—outside of China, people aren't going to rush to adopt a Chinese central—because it is the creepiest surveillance tool developed. They want to link it to a social credit system.

And, frankly, there are Western governments that are tripping over themselves to find ways to do the same thing. I think people should be alarmed that the Bank for International Settlements, the central banker to the central banks, is trying to develop protocols that are this creepy surveillance-state version.

What we should be studying—and we can't get the language adopted yet—would be—if we are going to study this with central banks, it would be, how do you do a true distributed-ledger, permissionless, peer-to-peer system if you are going to digitize money for your own currency?

Right now, the dollar is the dominant currency and likely will be for the foreseeable future. But the nature of that, how that is moved, people care about what does it translate to in dollars, even the most ubiquitous forms of central bank digital currency.

And I would say just one last observation, Mr. Redbord, on your comments. One is, if you kill the use cases for permissionless, peer-to-peer transactions because of your desire to corrupt money and turn it into a tool for control, you kill the use cases for all kinds of things that aren't meant to be payment systems.

So, I think it is an important thing that we protect that permissionless, peer-to-peer transaction system in all the ways that we talk about how to address our payment systems in the economy.

I wish we had more time. Thanks for having the hearing.

And thanks for your expertise. I would love to continue the dialogue with every one of you.

And I yield back.

Chairman HIMES. The gentleman's time has expired.

The gentleman from Ohio, Mr. Gonzalez, who is coming to us remotely, is now recognized for 5 minutes.

Mr. GONZALEZ OF OHIO. Thank you, Mr. Chairman. Thank you for holding this important hearing.

And thank you to our witnesses for your insights.

Mr. Redbord, I am going to start with you. There are some who believe that, absent a U.S. CBDC, we won't be able to implement sanctions or administer effective foreign policy. My contention is that private stablecoins, provided those coins are dollar-denominated and reserves are denominated in U.S. dollars, allow for sanctions to continue.

Where do you land on this specific question around the ability to conduct sanctions and foreign policy in a world of dollar-backed stablecoins versus a CBDC?

Mr. REDBORD. Thank you so much for the question.

I think there are two parts to this. I think, first, you have punitive sanctions measures. And we have seen those taken in the, sort of, private blockchain-based world. We have seen OFAC go after noncompliant exchanges, Russia-based, and essentially shut down their ability to move funds—ransomware payments, sanctions evasion. We have seen, as Mr. Levin and I both mentioned, them go after Lazarus Group, North Korea's cybercriminals, through the use of sanctions.

So, I think we have seen effective sanctions taken by OFAC in the private blockchain space already.

And then, I think the second piece of that is to really ensure that we are harnessing the power of, sort of the entrepreneurial spirit

in the United States to build a better mousetrap. And that is really where the importance of this committee and this institution come in, to really ensure that we are fostering innovation, that we are encouraging people to build.

And, as I mentioned in my opening statement, we are seeing today that 99 percent of stablecoins are—or stablecoins that are fiat-backed are tied to the U.S. dollar. And that means, already today, that we are ensuring that people who transact globally in this new digital system are transacting U.S. dollars, which really maintains the efficacy of U.S. sanctions, even in this new digital world where we keep hearing about the ability to move outside of the U.S. financial system.

Mr. GONZALEZ OF OHIO. Thank you. I could not agree more with that sentiment.

I want to shift now towards Tornado Cash, which, admittedly, I am still trying to wrap my head around fully. They were recently sanctioned by the Biden Administration on the logic that Tornado Cash is primarily a tool used by money launderers.

And I think the implication is twofold: one, that the technology—if you believe the Administration—is inherently evil and used for evil purposes. That is, sort of, one contention. And the second is that, once funds enter Tornado Cash, law enforcement becomes impossible or highly unlikely.

I want to take the second part first. Is it possible to still conduct law enforcement oversight and sanctions once funds enter a mixer like Tornado Cash?

Mr. LEVIN. I can take this, Congressman.

It is actually possible to follow funds through mixing services. And I know that sounds counterintuitive, but, in the case of the Ronin Bridge hack, we have just demonstrated that it is actually possible to seize funds on the other side of a mixing service.

It is not always possible; it is not always impossible. But it is actually a technology that Chainalysis has developed in order to be able to help law enforcement actually conduct those investigations.

Mr. GONZALEZ OF OHIO. Thank you.

And then back on—

Mr. REDBORD. If I could—

Mr. GONZALEZ OF OHIO. —the first point—quickly, on the first question, because I am running out of time, what legitimate uses might one have for using a mixing service? And I am thinking specifically about something like getting cryptocurrencies to Ukraine, but I don't want to preload that. But either of you can answer that.

Mr. REDBORD. Sure. That is a great example, Congressman.

But, also, in a world in which transactions are happening more and more in open blockchains, people are going to want a level of privacy. We see that people's cryptocurrency addresses have been made public through social media and other places. They are going to want to be able to transact with some level of privacy in those transactions. We see employers who may start paying in cryptocurrency, who know the various wallets they are sending funds into. Those people will want some level of privacy. You may want privacy from potential state surveillance.

But the reality is, I think the key to, sort of, the question around Tornado Cash is, as I thought Jonathan said very well, in terms

of the new capabilities of tools like TRM and Chainalysis to trace through mixers. But, also, it is important to ensure that regular users are not affected by these sanctions.

On the one hand, I think regulators are focused on going after illicit actors who are using these types of services, and, on the other hand, ensure that regular users are not being affected. And I think the key to that is having great data to really, really understand, sort of, what wallet addresses you are transacting with.

Mr. GONZALEZ OF OHIO. Thank you.

Privacy is a core American value. Let's not make it de facto illegal.

And, with that, I yield back.

Chairman HIMES. The gentleman's time has expired.

It would appear that we have no more Members with questions. Is that correct?

Okay.

I would like to thank our witnesses for their testimony today. This was a terrific conversation, as evidenced by the fact that every single member went over their time.

I think there remains a great deal of interest in following up on a lot of this, and we will certainly do that, including on some topics that we—obviously, the chairwoman has released some draft stablecoin legislation which will be fodder for a lot of consideration and thought. And I think there was also a desire, as you sensed, to look deeper into what, if any, a CBDC would make sense and what is the path there, if there is one.

So, again, I would like to thank all of our witnesses for their testimony.

The Chair notes that some Members may have additional questions for these witnesses, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

With that, I thank our witnesses one more time, and this hearing is adjourned.

[Whereupon, at 11:38 a.m., the hearing was adjourned.]

A P P E N D I X

September 20, 2022

House Financial Services Committee

Hearing entitled "Under the Radar: Alternative Payment Systems and the National Security Impacts of their Growth**"**
DATE: Tuesday, September 20th, 2022
TIME: 10:00 AM
LOCATION: Rayburn House Office Building, Room 2128
Prepared Testimony
Scott Dueweke
Global Fellow, The Wilson Center

Esteemed members of the House Financial Services Committee,

I am honored to be testifying before you today on the critical topic of the threat to national security posed by the use of virtual currencies. It is important to note that the scope of the term virtual currencies extends far beyond Bitcoin and other cryptocurrencies. These non-crypto alternative payment systems include many you are familiar with, such as PayPal, or WesternUnion. They also include hundreds more that you might not be familiar with such as the "dark PayPals" run by Russians including Webmoney and PerfectMoney. I previously testified before the Senate Judiciary Committee how the Russian QIWI system's co-branded Visa cards were used to purchase Facebook ads attempting to influence the 2016 US presidential election. By orders of magnitude, the largest of these non-crypto virtual currencies are China's centralized virtual currencies WeChat Pay and Alipay which processed 294.6 trillion yuan (US$45.6 trillion) in 2020. This dwarfs the $15.8T in crypto-related transactions in 2021.

By focusing only on cryptocurrencies we risk missing the forest for the trees. Indeed, there is a thriving ecosystem of virtual currencies, mobile payment systems, remittance systems, and stored value card systems. I define this as an ecosystem because they are all connected through hundreds of virtual currency exchanges willing to convert one alternative payment system for another. Anonymity or mis-attribution thrives here, with Know-Your-Customer (KYC) practices being poorly applied or ignored entirely, especially outside of the West.

The Alternative Payments Ecosystem provides an easy path for criminals and other adversaries of liberal democracies to bypass the checks and balances we have installed into the western financial system. As this non-bank system continues its rapid growth the threat of criminality and the destabilization of our monetary system dominance grows as well.

Thank you,

Scott Dueweke

SEPTEMBER 20, 2022

TESTIMONY BEFORE THE HOUSE FINANCIAL SERVICES COMMITTEE SUBCOMMITTEE ON NATIONAL SECURITY, INTERNATIONAL DEVELOPMENT, AND MONETARY POLICY

Hearing on Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth

Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth

BY

Emily Jin

Research Assistant
Energy, Economics, and Security Program
Center for a New American Security

Table of Contents

I. Introduction

Chairwoman Waters, Ranking Member McHenry, Subcommittee Chairman Himes, Subcommittee Ranking Member Barr, and the distinguished Members of the Subcommittee on National Security, International Development and Monetary Policy, thank you for the opportunity to testify before you on "Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth." It is an honor to share the panel with my fellow witnesses.[1]

My testimony will address China's progress in building out alternative payment systems, the strategic implications of growth in China's alternative payment systems, and recommendations for U.S. policymakers. The **key conclusion of this testimony** is:

> At their current stages, China's alternative payment systems are not threats to mainstream financial plumbing. However, these alternative payment systems are growing in technical sophistication and domestic adoption. China's Cross-Border Interbank Payment System (CIPS) and the eCNY (electronic Chinese yuan, or digital yuan) are making strides. CIPS' use is on an upward trajectory, and eCNY pilots are penetrating through all levels of Chinese society.
>
> Under an ambitious People's Republic of China (PRC) leadership that envisions more prominent roles for Chinese institutions in international finance, and with the right geopolitical winds, these systems could gain traction internationally and scale up accordingly. In such a scenario, Chinese alternative payment systems could eventually erode the effectiveness of U.S. and allied sanctions and challenge the institutions under the current financial order over the long run.

A summary of my **recommended plans for action**:

- Monitor the use, growth, and connectivity of these alternative payment rails with the rest of the world.
- Mandate U.S. government annual report on the use of the dollar in the context of global payment systems.
- Improve U.S. cross-border payments pipelines to make dollar transactions more efficient.
- Develop economic measures to restrict the advancement of alternative payment rails.
- Strengthen expertise in analyzing financial developments and statecraft.
- Draft a long-term strategy document (updated every two to four years) to signal the direction of U.S. financial statecraft and the administration's thinking for the future of the dollar.
- Engage proactively in standard setting bodies for digital assets and financial rails.

[1] This testimony reflects the personal views of the author alone. As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, the Center for a New American Security (CNAS) maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

The author would like to thank Emily Kilcrease, Yaya Fanusie, Alex Zerden, Elina Ribakova, Rachel Ziemba, Matthew Johnson, Martin Chorzempa, and Jonathon Sine for their assistance in developing the ideas in this testimony. The recommendations and views in this testimony, along with any errors, are the responsibility of the author alone.

II. China's Alternatives for a Multi-Polar Financial Order

HOW CIPS CAPTURED GLOBAL IMAGINATION

The Russian invasion of Ukraine upended the international community's assumption about how economic interconnectedness brings geopolitical stability. Western sanctions on Russia in response to its invasion of Ukraine has called attention to the fundamental way international finance operates, and brought to the fore the otherwise under-studied pipes of the international financial system. While China has been developing its alternative payment systems for some time, Russia's war in Ukraine has focused concern on the development of these alternative payment channels. The United State and allied countries leveraged their economic and financial power to exclude Russia from global financial pipes, via an unprecedented package of sanctions on the Central Bank of Russia and other major Russian banks, which cut Russia off from accessing assets denominated in currencies that add up to 95 percent of global foreign exchange reserves.[2] This vacuum provided significant incentives for China to potentially come to the aid of Russia. Moreover, it created space for all other countries that are in the "messy middle" (not explicitly taking either Ukraine or Russia's side), which are left having to decide whether to cooperate with the United States and some European and Indo-Pacific allies, abstain from action, or provide tacit endorsement or support to Russia.[3]

The oft-mentioned analogy of payments systems being the plumbing of international finance is apt. To participate in global finance, financial institutions such as banks benefit from the Society for Worldwide Interbank Financial Telecommunications (SWIFT), which provides secure messaging to facilitate and ensure timely and cheap means of transferring value around the world. Message-facilitated communications and the actual movement of money and value are separate, and SWIFT only does the former. It has a robust membership of more than 11,000 participating institutions around the world in 200 countries, and is co-owned by over 2,000 banks and governed by a board of global financial executives. It is a crucial valve in the international financial ecosystem. Cross-border payments are usually conducted with the correspondent banking model, where transactions pass through multiple intermediary banks [with the payment communicated through SWIFT at each step] before reaching its final destination account. Along with the rapid globalization in the past few decades, the payments world had to adapt and adjust to the challenges in cross-border payments, which often entail currency conversions, and varied tax regimes, and processing fees. SWIFT, as the most prominent pipe in international payments, passed 42 million messages per day in between global financial institutions in 2021.[4] To move value around the world without SWIFT would be challenging.[5]

In addition to central bank sanctions, the United States and allies worked together to block Russia from a major part of global financial plumbing via sanctions applicable to the Belgium-based SWIFT.[6] What happens when one part of

---

[2] Emily Kilcrease, Jason Bartlett, Mason Wong, "Sanctions by the Numbers: Economic Measures against Russia Following its 2022 Invasion of Ukraine," Center for a New American Security, https://www.cnas.org/publications/reports/sanctions-by-the-numbers-economic-measures-against-russia-following-its-2021-invasion-of-ukraine.

[3] Carisa Nietsche, 'The 'Messy Middle'," *The New York Times*, April 18, 2022, https://www.cnas.org/press/in-the-news/the-messy-middle.

[4] Shobhit Seth, "How the SWIFT Banking System Works," Investopedia, https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp.

[5] Seth, "How the SWIFT Banking System Works."

[6] Specifically, two days after the Russian invasion of Ukraine, the allies brought upon coordinated sanctions on seven major Russian banks--VTB Bank, Bank Otkritie, Novikombank, Promsvyazbank, Rossiya Bank, Sovcombank, and VEB—in the form of SWIFT sanctions. Read more at Emily Kilcrease, Jason Bartlett, Mason Wong, "Sanctions by the Numbers: Economic Measures against Russia Following its 2022 Invasion of Ukraine," Center for a New American Security, https://www.cnas.org/publications/reports/sanctions-by-the-numbers-economic-measures-against-russia-following-its-2021-invasion-of-ukraine. The United States, the United Kingdom, Japan, and other countries have supported the disconnection of certain other Russian financial firms from SWIFT including the larger State-owned banks, read more at "Statement by Press Secretary Jen Psaki on Japan's Announcement to Hold Russia Accountable", February 27, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/27/statement-by-press-secretary-jen-psaki-on-japans-announcement-to-hold-russia-accountable/. One thing to note is this action excluded Gazprombank, which was intended to leave room for energy-related transactions and payments, read more at Philip Blenkinsop, "EU Bars 7 Russian Banks from SWIFT, but Spares Those in Energy," Reuters, March 2, 2022, https://www.reuters.com/business/finance/eu-excludes-seven-russian-banks-swift-official-journal-2022-03-02/. Euro- and dollar-denominated payments would continue to allow for transactions involving Russia's most lucrative exports, but still faced restrictions on setting up correspondent banking accounts and required additional steps to conduct the transactions. Read more at Robert Greene, "How Sanctions on Russia Will Alter Global Payments Flows," Carnegie Endowment for International Peace, March 4, 2022, https://carnegieendowment.org/2022/03/04/how-sanctions-on-russia-will-alter-global-payments-flows-pub-86575.

the international financial plumbing is unavailable to a country's financial institutions? Economic and financial actors like businesses and banks naturally look to alternative financial systems and see whether those could fill the gap. As a result, attention turned to China's CIPS.[7] CIPS is China's international-facing RMB clearing and settlement system (clearing entails movement of funds from institution A to institution B, and settlement is the finalization of moved funds). Observers have wondered whether CIPS and other Chinese channels could provide a replacement for SWIFT not just for trade with China, but also for transactions with other countries that do not involve China.[8] Moreover, the Russia sanctions created a strategic incentive for China to strengthen its alternative payment systems for its own sake. Chinese scholars and policymakers alike are cognizant that China, given its intentions with regards to Taiwan, may one day be cut off from global financial plumbing.[9] A group of Chinese academics and practitioners argued in an August 2022 article that China needs to hedge the risk of financial sanctions by promoting RMB-denominated finance and enhancing China's role in the SWIFT network.[10] The former governor of the PBOC (2002-2018) remarked in 2022 that CIPS cannot easily replace SWIFT given it is mainly an RMB clearing and settlement institution as opposed to a messaging system. However, as this group argues, the impact of SWIFT sanctions may "necessitate any target economy to prop up their alternative payment rails."[11]

Congressional action is commensurate with public concern. Senators Marco Rubio (R-FL), Rick Scott (R-FL), and Todd Young (R-IN) have introduced legislation related to China's CIPS, namely the Crippling Unhinged Russian Belligerence and Chinese Involvement in Putin's Schemes (CURB CIPS) Act.[12] The proposed the legislation would "freeze or terminate any U.S.-based accounts connected to Chinese financial institutions – or block the U.S.-based property of such institutions – that engage in transactions with a Russian financial institution using either CIPS or SPFS."[13] Another related proposed legislation by Representative Hill (R-Ark.)—Special Drawing Rights Oversight Act—would introduce congressional oversight on the executive branch (via the Department of the Treasury) in approving Special Drawing Rights (SDR) funding for the International Monetary Fund.[14] SDRs are international reserve assets that supplement official reserves of IMF member countries, and are based on a basket of five currencies (the U.S. dollar, the euro, the Chinese RMB, the Japanese yen, and the British pound sterling).[15] The intention behind this proposed legislation is to prevent Russia from converting their share of the SDRs to Chinese renminbi (RMB) by exchanging its SDRs with China for RMB reserves. Mirroring congressional concerns, H.R. McMaster, national

---

[7] "Factbox: What is China's Onshore Yuan Clearing and Settlement System CIPS?" Reuters, February 28, 2022, https://www.reuters.com/markets/europe/what-is-chinas-onshore-yuan-clearing-settlement-system-cips-2022-02-28/.

[8] Kandy Wong, Ji Siqi, https://www.scmp.com/economy/global-economy/article/3168829/ukraine-invasion-swift-ban-sanctions-cut-russian-economy

[9] Cissy Zhou, "China Scrambles for Cover from West's Financial Weapons," Nikkei Asia, April 13, 2022, https://asia.nikkei.com/Spotlight/The-Big-Story/China-scrambles-for-cover-from-West-s-financial-weapons.

[10] Ba Shusong, "巴曙松：人民币跨境支付系统（CIPS）与 SWIFT 的协同发展 [Coordinated Development of RMB Cross-Border Payment System (CIPS) and SWIFT]," Sina, https://web.archive.org/web/20220919121045/https://finance.sina.cn/forex/hsxw/2022-09-01/detail-imizmscv6698997.d.html?vt=4&cid=76601&node_id=76601.

[11] Yanting Mai, "唱反调：周小川指人民币 CIPS 难以取代 SWIFT 促勿令国际支付系统作冷战 [Zhou Xiaochuan Says It's Difficult to Replace SWIFT with RMB CIPS, Urge Not to Make International Payment System a Cold War]," Radio France Internationale (RFI), April 18, 2022, https://web.archive.org/web/20220919004954/https://www.rfi.fr/cn/%E4%B8%AD%E5%9B%BD/20220418-%E5%94%B1%E5%8F%8D%E8%B0%83-%E5%91%A8%E5%B0%8F%E5%B7%9D%E6%8C%87%E4%BA%BA%E6%B0%91%E5%B8%81-cips-%E9%9A%BE%E4%BB%A5%E5%8F%96%E4%BB%A3-swift-%E4%BF%83%E5%8B%BF%E4%BB%A4%E5%9B%BD%E9%99%85%E6%94%AF%E4%BB%98%E7%B3%BB%E7%BB%9F%E4%BD%9C%E5%86%B7%E6%88%98.

[12] "Rubio, Colleagues Introduce Bill to Prevent Russia-China Financial Coordination," March 17, 2022, https://www.rubio.senate.gov/public/index.cfm/press-releases?id=B590BC13-D6AE-4C43-99CE-ACE1996E013C; U.S. Senate, *Crippling Unhinged Russian Belligerence and Chinese Involvement in Putin's Schemes Act o* 2022, 117t Cong., https://www.rubio.senate.gov/public/_cache/files/54287803-ca01-4396-a5ff-edf8900163b9/68D57AB15BCAFBCD96CBF3AC6B170674.ros22312.pdf.

[13] "Rubio, Colleagues Introduce Bill to Prevent Russia-China Financial Coordination," March 17, 2022, https://www.rubio.senate.gov/public/index.cfm/press-releases?id=B590BC13-D6AE-4C43-99CE-ACE1996E013C.

[14] "Rep. Hill Introduces Bill to Stop Democrats' Blank Check to Genocidal Regimes and State Sponsors of Terrorism," March 5, 2021, https://hill.house.gov/news/documentsingle.aspx?DocumentID=8315.

[15] "Fact Sheet: The Role of the SDR," IMF, July 29, 2022, https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR#:~:text=The%20value%20of%20the%20SDR,and%20the%20British%20pound%20sterling.

security advisor under President Donald Trump, remarked at a Hoover Institution event that "to get at Russia, there are elements of our policies that have to touch China."[16]

CIPS: AN ALTERNATIVE SYSTEM

The Cross-Border Interbank Payments Systems (CIPS) was conceived as a project in 2012, launched into development in 2015, and connected the Mainland and Hong Kong stock markets to become a major RMB cross-border settlement channel in 2017.[17] It is based in Shanghai, with ownership stakes by state-owned banks, exchanges, and Western banks, and falls under the supervision of China's central bank, the People's Bank of China (PBOC).[18] According to a presentation deck by the PBOC's Payment and Settlement Division Research Office, prior to CIPS, RMB cross-border transactions were, prior to CIPS, conducted in three ways—via correspondent banks, via clearing banks, and via non-resident accounts (accounts opened by an institution legally incorporated and registered overseas, such as Hong Kong).[19] Under the correspondent bank model, an offshore bank signs an agreement with a commercial Chinese bank that offers international settlement services, which allows the offshore bank to open an RMB account with the Chinese bank and access the Chinese domestic payment system. An illustrative example would be JP Morgan opening a correspondent account at the Bank of China, which then allows JP Morgan clients with business in China to take the U.S. dollar in their JP Morgan account and transfer it into RMB, then to an exporter's Chinese bank account. The clearing bank model differs in that it provides participating offshore banks with RMB through accounts held at the offshore RMB clearing banks. The non-resident accounts (NRA) model offers foreign companies the opportunity to open bank accounts in China. The PBOC explicitly stated CIPS was created principally to meet increasing demands and streamline the processes of cross-border RMB settlement.[20]

China's banking system implements two payment systems—the China National Advanced Payment System (CNAPS), which facilitates domestic RMB clearing and settlement, and the Cross-Border Interbank Payment System (CIPS), which facilitates cross-border RMB clearing and settlement.[21] CIPS is connected with other domestic Chinese interbank payment systems, including the High-Value Payment System (HVPS, which is a real-time gross settlement system for large volume transactions), the Bulk Electronic Payment System (BEPS), the Cheque Image System (CIS), the Internet Banking Payment System (BIPS) and the China Domestic Foreign Currency Payment System (CDFCPS).[22] For the purposes of this hearing, CIPS should be the focus as it is the gateway for majority of foreign financial institutions and companies that want access to streamlined to international clearing and settlement of the RMB. It works by facilitating payment orders between correspondent accounts of financial institutions. Foreign financial institutions are generally indirect participants with CIPS, while Chinese financial institutions and some foreign bank's Chinese branches are direct participants.[23] The difference between indirect and direct participation is direct participation allows institutions to directly send and receive messages through CIPS, whereas indirect

---

[16] Phelim Kine, China Watcher Newsletter, POLITICO, March 24, 2022, https://www.politico.com/newsletters/politico-china-watcher/2022/03/24/chinas-russia-embrace-triggers-congress-blowback-00019936; https://hill.house.gov/news/documentsingle.aspx?DocumentID=8315.

[17] "人民币跨境支付系统(CIPS) 主要功能及业务管理 [RMB Cross-Border Payment System (CIPS) Main Functions and Business Management]," Research and Planning Office of the Payment and Settlement Division – People's Bank of China, July 2018, https://web.archive.org/web/20220405135004/https://res.cocolian.cn/pbc/%E4%BA%BA%E6%B0%91%E5%B8%81%E8%B7%A8%E5%A2%83%E6%94%AF%E4%BB%98%E7%B3%BB%E7%BB%9FCIPS%E4%B8%9A%E5%8A%A1%E7%AE%A1%E7%90%86%E5%88%B6%E5%BA%A6%E4%BB%8B%E7%BB%8D-201807.pdf, 3.

[18] Steve Murphy, "Skirting Russian Sanctions with China's CIPS? Not So Fast," PaymentsJournal, March 15, 2022, https://www.paymentsjournal.com/skirting-russian-sanctions-with-chinas-cips-not-so-fast/.

[19] "人民币跨境支付系统(CIPS) 主要功能及业务管理 [RMB Cross-Border Payment System (CIPS) Main Functions and Business Management]," Research and Planning Office of the Payment and Settlement Division – People's Bank of China, 4.

[20] "人民币跨境支付系统(CIPS) 主要功能及业务管理 [RMB Cross-Border Payment System (CIPS) Main Functions and Business Management]," Research and Planning Office of the Payment and Settlement Division – People's Bank of China, 8.

[21] Alternative for CIPS include China International Payment System, and China Interbank Payment System, read more at Béatrice Ozanne, "What is CIPS Onshore Yuan Clearing & Settlement?" Statrys, https://statrys.com/blog/cnips-code.

[22] "Payment, Clearing and Settlement Systems in China," Bank for International Settlements, 2012, https://www.bis.org/cpmi/publ/d105_cn.pdf.

[23] "RMB Cross-Border Interbank Payment System," Mizuho Group, December 5, 2017, https://www.mizuhogroup.com/binaries/content/assets/pdf/mizuho-bank/cips.pdf; "直接参与者名单 - 76 家 直接参与者（截至 2022 年 6 月） [List of Direct Participants – 76 Direct Participants as of June 2022]," https://www.cips.com.cn/cips/gywm/cipsxt/zjcyzmd/index.html.

participation require institutions to send messages with direct participating banks via SWIFT (a parallel with the traditional correspondent banking model).[24] As of now, foreign financial institutions (with the exception of some of their Chinese branches) are only indirect participants of China's CIPS. This is likely due to the fact that direct participation in CIPS would erode the PBOC's control over offshore usage of the RMB.[25]

Instead of drawing similarities between China's CIPS and SWIFT, it is more apt to liken China's CIPS to the Clearing House Interbank Payments System (CHIPS), which is the largest private sector USD clearing system in the world. CIPS and SWIFT have different mechanics and were created in different contexts. Technically, CIPS clears and settles RMB transactions, whereas SWIFT is a secured messaging protocol that lets banks "talk" to one another, facilitating but not concluding the transactions. Contextually, CIPS was created to improve the efficiency of RMB transactions, whereas SWIFT was created by institutions from the U.S., the European Union, and G7 countries to enhance global financial messaging. To say the two are peers would be misleading, given that CIPS relies on SWIFT to conduct a majority of its international settlements (see below for a scenario of CIPS and SWIFT usage).[26] The only way CIPS is similar to SWIFT is in its networking capability. For SWIFT, it connects global financial institutions to each other, whereas CIPS connects mostly domestic Chinese payment systems with one another.

	SWIFT	CIPS	SPFS [27]
What It Does	Launched in 1977 to ensure secure messaging between global financial institutions. It facilitates movement of funds, but does not move funds itself.	Established in 2015 to clear and settle onshore and offshore RMB transactions. It moves funds by using SWIFT-enabled messaging.	Established by the Bank of Russia in 2014. It facilitates movement of funds within Russia.
Why It Was Created	To standardize interbank communications, which improves efficiency and lowers the costs of transactions.	To increase the efficiency and lower the costs of RMB transactions.	To ensure transactions take place without the need to go through SWIFT.
Participants	11,000+ participating institutions in 200 countries.	1,341 participating institutions in 103 countries.	400+ participating institutions.
Volume of Trade Processed	$140 trillion annually [28]	$12.68 trillion in 2021 [29]	$1.73 billion in 2020 [30]

Author's Table, originally published in Lawfare on April 5, 2022, with additional details.

How Transactions Work through SWIFT. In the scenario where user A wants to send funds to user B across borders, if their banks are in the SWIFT network, their banks can communicate with one another via SWIFT codes to complete the transaction. If one of their banks are not in the SWIFT network, then the transaction will need to go through correspondent (intermediary) banks in the SWIFT network, which increases the time and cost of the transaction.

[24] Zhou, "China Scrambles for Cover from West's Financial Weapons," *Nikkei Asia*.

[25] Zhou, "China Scrambles for Cover from West's Financial Weapons," *Nikkei Asia*.

[26] Todd C. Lee, "China (Mainland) May Move to Limit Impact of US Financial Weapons," HIS Markit, May 4, 2022, https://ihsmarkit.com/research-analysis/china-may-move-to-limit-impact-of-us-financial-weapons.html.

[27] Author added this SPFS column for comparison, though the thrust of this testimony focuses on CIPS, not SPFS.

[28] Greene, "How Sanctions on Russia Will Alter Global Payments Flows," Carnegie Endowment for International Peace.

[29] This $12.68 trillion processed in 2021 was a 75 percent increase from the year before. This number was sourced from *Jiefang Daily*, the newspaper of the People's Liberation Army, so this statistic should be understood in the context of state propaganda.

[30] "Transaction Volume of Different Domestic and Cross-Border Elements in Russia's Payment System from 2012 to 2020 (in millions)," Statista, https://www.statista.com/statistics/1293287/market-size-of-different-payment-systems-in-russia/.

In comparison, CIPS is different from SWIFT as it is an RMB clearing and settling institution that more often than not utilizes SWIFT to facilitate RMB transactions with the rest of the world.

A → A's Bank { A & B's banks = no relationship → Intermediary banks → B
A & B's banks = yes relationship, go through **SWIFT** → B

CIPS as an RMB clearing and settling house
Plugs into SWIFT and uses its messaging to connect with global finance

***Author's Visual Rendition.*

Notably, CIPS processed around 80 trillion yuan ($12.68 trillion) in 2021, a 75 percent increase from a year ago, according to state-backed newspaper *Jiefang Daily*.[31] As of end-January 2022, CIPS said about 1,280 financial institutions in 103 countries and regions have connected to the system. This $12.68 trillion in processed volume in 2021 still pales in comparison to the $140 trillion processed annually via SWIFT. **In the near term, this trend is not changing.** The United States occupies a preponderant role within international finance, as it makes up 59 percent of foreign exchange reserves, and more than 80 percent of foreign exchange transactions occur against the U.S. dollar.[32] The attractiveness of the American economic and financial environment, underwritten by a political economic system founded on rule of law, translates to currency attractiveness. These structural advantages are not changing anytime soon.

Nevertheless, policymakers should be wary of the strategic implications behind a strengthened CIPS. If more foreign banks decide to participate in CIPS, it could elevate the attractiveness of the institution to more banks and quickly expand market share. Even though a majority of CIPS' transactions require SWIFT to facilitate the messaging, there seems to be mechanisms within the CIPS that allow for RMB clearing and settlement without SWIFT. According to the same deck from the PBOC Payments and Settlement Department, the CIPS system has the following structure:

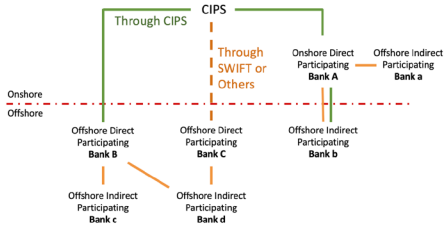


Figure: Author recreation from p. 22 of PBOC's 2018 Presentation on CIPS. In some cases, CIPS can operate through its own special channels without going through SWIFT.

[31] "在全球范围内 越来越多的人正在采用上海推出的金融标准 [Globally, More People are Adopting the Financial Standards Introduced by Shanghai]," *Jiefang* Daily, February 28, 2022, https://web.archive.org/web/20220919083115/http://sh.news.cn/2022-02/28/c_1310491783.htm.
[32] "US Dollar Funding: An International Perspective," Working Group Chaired by Sally Davies and Christopher Kent – Bank for International Settlements, June 2020, https://www.bis.org/publ/cgfs65.pdf.

CIPS seems to mandate direct participating financial institutions' involvement for RMB clearing and settlement that do not go through SWIFT messaging.

The PBOC likely has plans to enhance the functionality of CIPS so that it will eventually rely on SWIFT less. Out of the basic principles behind CIPS, the PBOC specific that CIPS functionality will be conducive to isolating legal risks in cross-border payment settlement and creating a fair competitive environment.[33] Given the "neutrality" critique on SWIFT especially among waves of financial sanctions on Russia, this seems deliberate on China's part to create a payment system that espouses principles of fairness. The PBOC has intentions to normalize the use of RMB clearing and settlement via CIPS from its 2018 presentation (see below). The orange dashed lines indicate CIPS are transacting with financial institutions in North and South American jurisdictions via SWIFT. The yellow solid lines likely indicate China aims to circumvent SWIFT messaging and settle RMB transactions directly with financial institutions in these regions. How the PRC intends to achieve just that is unclear, but the intention is apparent.

Figure: Pg. 22 of the PBOC's 2018 Presentation on CIPS.

ECNY: AN ALTERNATIVE RAIL

How do central bank digital currencies (CBDC) factor into the alternative payment system calculus? China has been expanding pilots to integrate its eCNY into its economic infrastructure.[34] In a previous Center for a New American Security report, the authors concluded that the PRC is first and foremost preoccupied with getting the domestic

[33] "人民币跨境支付系统(CIPS) 主要功能及业务管理 [RMB Cross-Border Payment System (CIPS) Main Functions and Business Management]," Research and Planning Office of the Payment and Settlement Division – People's Bank of China, 8.
[34] Yaya Fanusie, Emily Jin, "China's Making Smart Money," *Lawfare*, September 15, 2021, https://www.lawfareblog.com/china-making-smart-money.

application of eCNY right.[35] In state planning documents such as the July 2021 PBOC white paper on China's progress in developing its central bank digital currency, the PBOC wants to facilitate the use and adoption of eCNY domestically to better inform Chinese policymakers on the Chinese economy and citizenry.[36] The domestic surveillance implications are concerning, and these concerns could extend to cross border scenarios down the line. That are various potential cross-border applications of the eCNY. Over the short to medium term, PBOC is conducting a cross-border CBDC-to-CBDC proof of concept through the Bank for International Settlements' (BIS) project, the mCBDC (multi-CBDC) bridge.[37] Over the long term, China is looking to advance global CBDC standards.

While these efforts are still in nascent stages, they point to a roadmap where China seeks an alternative cross-border system buttressed along CBDC rails, and where China is a major influencer of how those rails are constructed and managed. Also, an alternative stem for CBDC for international value transfer is not the desire of U.S. adversaries alone seeking ways along around US sanctions.[38] U.S. allies are exploring and piloting CBDCs.[39] The former Bank of England governor Mark Carney called in 2019 for a digital alternative to the U.S. dollar, specifically taking the form of a digital currency supported by an international coalition of central banks.[40] In fact, the Bank for International Settlements—whose membership includes 63 central banks—produced a report earlier this year that envisions sovereign digital currencies as the future of global banking.[41] One thing to note is the mCBDC bridge is not facilitating eCNY transactions (which are mostly retail at the current stage), but is modeling a wholesale CBDC system involving payments between global banks. While this is a separate stream of CBDC piloting, it fits into China's overall push to build alternative financial rails for retail and institutional RMB transactions.

The PBOC is conducting tests for non-PRC mainland use of the eCNY. Hong Kong Monetary Authority (Hong Kong's central bank) Vice President Li Dazhi announced that the an eCNY cross-border pilot technical test has entered its second stage, which entails streamlining payments through eCNY wallets.[42] Hong Kong is the first cross-border eCNY pilot to conduct technical tests in cooperation with the PBOC's Digital Currency Research Institute. Li explicitly stated that the hope is for "multiple digital renminbi operators and local banks" to "participate in the test so that Hong Kong residents can use the digital renminbi on the mainland in the future." Besides areas like Hong Kong, China is also projecting its designs for countries in its regional backyard. Most recently at the Shanghai Cooperation Organization September gathering, General Secretary Xi mentioned China will be developing cross-border payment and settlement systems (in local currencies) for Central Asian countries.[43] While he did not explicitly mention the eCNY, it is safe to assume the PRC leadership would eventually want the eCNY to be adopted in Central Asia if not the rest of the region.

All indications point to the likelihood that U.S. and other foreign multinational corporations will be compelled to accept eCNY payments for retail transactions in China. McDonalds integrated the eCNY payments option into their

---

[35] Yaya Fanusie, Emily Jin, "China's Digital Currency: Adding Financial Data to Digital Authoritarianism," (Center for a New American Security, January 26, 2021), https://www.cnas.org/publications/reports/chinas-digital-currency.
[36] "Progress of Research & Development of E-CNY in China," Working Group on E-CNY Research and Development of the People's Bank of China, July 2021, http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.
[37] Bank for International Settlements, "Multiple CBDC (mCBDC) Bridge," https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.
[38] Yaya J. Fanusie, Trevor Logan, "Crypto Rogues: U.S. State Adversaries Seeking Blockchain Sanctions Resistance," (The Foundation for Defense of Democracies), July 11, 2019, https://www.fdd.org/analysis/2019/07/11/crypto-rogues/.
[39] Bank for International Settlements, "BIS Innovation Hub Work on Central Bank Digital Currency (CBDC)," https://www.bis.org/about/bisih/topics/cbdc.htm.
[40] Nikhilesh De, "UK Central Bank Chief Sees Digital Currency Displacing US Dollar as Global Reserve," August 23, 2019, https://www.coindesk.com/markets/2019/08/23/uk-central-bank-chief-sees-digital-currency-displacing-us-dollar-as-global-reserve/.
[41] "The BIS Presents a Vision for the Future Monetary System," June 21, 2022, https://www.bis.org/press/p220621.htm.
[42] "香港转数快测试数字人民币充值，范围和规模扩大 [Hong Kong FPS Tests Digital RMB Recharge, Expanding Scope and Scale]," MPaypass, September 13, 2022, https://web.archive.org/save/https://www.mpaypass.com.cn/news/202209/13100349.html.
[43] "Full Text of Xi's Speech at SCO Samarkand Summit," Xinhua, September 16, 2022, https://english.news.cn/20220916/9a25ddd0a86848a09ef0b2a4e499a52d/c.html.

applications and restaurant locations.[44] Businesses will likely need to choose whether to honor their profitability by facilitating eCNY transactions, or bow out of a significant part of the Chinese market by abstaining from eCNY.

The eCNY seems to be running on a different architecture than CIPS. International banks have been applying to be integrated as part of the eCNY clearing system (such as HSBC). It would only make sense that the PRC would want more foreign participating financial institutions in its eCNY infrastructure to facilitate usage of its digital sovereign currency.[45] Eventually, the PBOC might want to explore interoperable connections between CIPS and the eCNY systems.

What are Beijing's intentions for implementing the eCNY? A useful heuristic is the concept of *legibility*, which measures the extent to which one can make sense of complex realities with simplifying metrics.[46] A state's ability to parse the activities and behavior of its populace is a prerequisite to the state leveraging its populace as a resource to accrue national power. Through the eCNY, the PRC intends to collect as much data on its populace as possible. If it successfully leverages collected information to promote economic growth and enact tighter social control, the People's Republic of China would become the People's Republic of Digital Legibility. The PRC also wants to streamline international payments with the eCNY. While almost everyone is connected to the United States and its dollar infrastructure, not everyone is connected to each other. This tends to lead to inefficient payment processes. With CBDCs and initiatives like mCBDC bridge, central banks and other financial institutions may connect with one another and not need to go through U.S. dollar anymore as the vehicle currency.

CONDITIONS FOR CHINESE ALTERNATIVES TO GAIN TRACTION

However, for Chinese alternative payments systems such as CIPS and eCNY to gain traction, the RMB would need to become a reliable medium of exchange and store of value. Currently, the RMB is not considered a safe asset, as its state control political and economic model does not lend to investor confidence. Immense privileges and responsibilities stem from issuing and overseeing a major currency. The United States provides the world's deepest capital market due to the tradability and convertibility of its desirable currency. The United States' open accounts are burdened with imbalances imported from the rest of the world.[47] The social and economic burden of maintaining a major global currency is currently unthinkable for the PRC. The PRC cannot afford to have an appreciating RMB, which would be detrimental to its export-reliant economic model. It also cannot afford an unrestricted capital account inside of Mainland China and increasingly in the offshore RMB market in Hong Kong given fear of capital flight and instability.[48]

Moreover, China needs to stay plugged into mainstream financial plumbing offered by SWIFT. CIPS itself relies on SWIFT in transacting in RMB with the rest of the world. China relies on the U.S. dollar to conduct trade. Even though the RMB is technically the fifth most used currency in international payments, it lags the U.S. dollar, the Euro, the Japanese Yen, and the British Pound Sterling at 2 percent of international payments. Similarly, it hovers around 2 percent in its share of global foreign exchange reserves held in RMB-denominated assets.[49] While China is developing CIPS and other alternative financial institutions, it also wants to reap the benefit of participation in the Western-led

---

[44] Demetri Sevastopulo, Andrew Edgecliffe-Johnson, Ryan McMorrow, Edward White, "China Presses McDonald's to Expand e-Currency System Before Olympics," *Financial Times*, October 20, 2021, https://www.ft.com/content/1f4274f4-b914-4534-89c0-62b9b7763f2b.

[45] "数字人民币大幅扩围！城银清算、农信银协助多家银行接入 [The Digital Renminbi has Expanded Significantly! City Bank Clearing and Rural Credit Bank Assist Multiple Banks in Access]," August 13, 2021, https://web.archive.org/save/https://www.mpaypass.com.cn/news/202108/13201231.html; Noel Quinn, "New Forms of Digital Money Could Spur Growth," HSBC, September 20, 2021, https://www.hsbc.com/insight/topics/new-forms-of-digital-money-could-spur-growth.

[46] James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (1998), https://yalebooks.yale.edu/book/9780300078152/seeing-like-a-state/.

[47] "Remarks by Governor Ben S. Bernanke," The Federal Reserve Board, April 14, 2005, https://www.federalreserve.gov/boarddocs/speeches/2005/200503102/

[48] Joseph W. Sullvan, "Don't Discount the Dollar Yet," Foreign Policy, https://foreignpolicy.com/2020/08/21/dollar-global-reserve-currency-yuan-china/.

[49] Eswar Prasad, "The Renminbi Rises but Will Not Rival the Dollar," Brookings Institution, October 2020, https://www.brookings.edu/articles/the-renminbi-rises-but-will-not-rival-the-dollar/.

financial order. In fact, China does not want to be excluded from the international financial system. A researcher at the Chinese Academy of Social Sciences posited in his article that China should strive to become "too connected (with international finance) to fail," which is a nod to the benefits of participation in a dollar-dominant financial order.[50]

But over the long term, foreign participation in CIPS might be an indicator of China's growing financial power. It may alter long-term trends of global payment flows, especially if CIPS technically gains and refines SWIFT-like capability down the line, which is potentially achievable given SWIFT's joint venture with the PBOC's digital currency research institute and clearing center in 2021.[51] The PBOC has set up bilateral swaps with BRICS countries since 2013, which are agreements where participating central banks agree on using their own currencies to settle bilateral trade. This is a non-negligible foundation for a non-dollar dominant future. [52] If eCNY developers are successful at implementing the "programmability" (smart contract capability within the digital currency) of the digital currency, the PRC may be more willing to open up partially its capital account, which could lead to partial political economic liberalization and increased attractiveness of the RMB.[53]

China has very clear ambitions in leading in international finance in the future, as specified in the Financial Standardization Five Year Plan (2021-2025) released in February 2022, where it espoused aspirations to create and shape standards in global finance.[54] Major Chinese government agencies with financial mandates would be implementing this plan, including the People's Bank of China, the State Administration for Market Regulation, China Banking and Insurance Regulatory Commission, and China Securities Regulatory Commission. This whole-of-Chinese-bureaucracy effort clearly signals China's ambition to shape international finance in the future.

[50] Qiyuan Xu of the Institute of World Economics and Politics at the Chinese Academy of Social Sciences discusses in his July 2021 (check date) article that while the likelihood of the United States influencing SWIFT to sanction Hong Kong and the Mainland is small, the likelihood of SWIFT sanctions being imposed on individual financial institutions inside of China or Hong Kong are increasing. He said to respond to this possibility, China should try to ensure its institutions are "too connected to fail (太关联而不能倒)," which the author take to be an indication that some experts inside China are advocating for China to be more interwoven into the international financial system.

[51] Update 1-SWIFT Sets Up JV with China's Central Bank," Reuters, February 4, 2021, https://www.reuters.com/article/china-swift-pboc/update-1-swift-sets-up-jv-with-chinas-central-bank-idUSL1N2KA0MS

[52] Agnieszka Flak, Marina Lopes, "China, Brazil Sign Trade, Currency Deal Before BRICS Summit," Reuters, March 26, 2013, https://www.reuters.com/article/uk-brics-summit/china-brazil-sign-trade-currency-deal-before-brics-summit-idUKBRE92P0FT20130326.

[53] "The Digital Yuan Offers China a Way to Dodge the Dollar," *The Economist*, September 5, 2022, https://www.economist.com/finance-and-economics/2022/09/05/the-digital-yuan-offers-china-a-way-to-dodge-the-dollar?utm_medium=cpc.adword.pd&utm_source=google&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-

[54] "金融标准化"十四五"发展规划 [The Financial Standardization Five Year Plan (2021-2025)], January 2021, https://web.archive.org/web/20220919081344/http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4467138/20220208183748453 11.pdf.

III. The Global Financial Order is Still Uni-Polar

YES, DE-DOLLARIZTION IS AFOOT IN CHINA AND RUSSIA

There are certainly economic and financial forces at play in China-Russia relations that point to clear intentions to reduce their reliance on the U.S. dollar. For example, Russia signed 38 agreements with China in 2014, some of which established a three-year currency swap deal with 130 billion yuan.[55] Since 2019, Beijing and Moscow have replaced the dollar with their own currencies to settle bilateral trades. Russia's exports denomination in dollar was reduced from 80 percent in 2013 to less than half as of March 2022.[56] In 2022, China's exports to the United States shrank for the first time in the last two years while shipments to Russia surged, likely due to Chinese brands filling the void of Western brands that departed Russia.[57]

Both China and Russia have been de-dollarizing for some time on their own. China has reduced its holdings of U.S. dollar reserves from 79 percent of its total foreign exchange reserves in 1995 to 59 percent in 2016.[58] It has set up offshore RMB trading locations in Hong Kong, Singapore, and Europe to denominate trades in RMB. That, combined with China's efforts to incorporating foreign exchange and RMB in cross-border financing point to aspirations in de-dollarization.[59]

Similar trends have been carried out in Russia with more intensity and urgency. Russia has been de-dollarizing since 2014. It has reduced its own holdings of the dollar (Russian Central Bank's stockpile) from 40 percent in 2017 in to 16 percent in 2021.[60] In July 2021, the Russian finance minister announced plans to remove dollar-denominated assets from Russia's sovereign wealth fund, which was a third of the $186 billion fund.[61] It has also developed payment processing capabilities to reduce reliance on dollar-centered payments infrastructure. The Mir cards were created precisely to respond to U.S.-led global payment processing ecosystem denying services to Russian banks under U.S. sanctions after Russia's first invasion of Ukraine in 2014. After Visa, Mastercard, and China's UnionPay backed out of Russia in May 2022, Mir cards increased their adoption among both domestic and international audiences, though the international user base is limited to a couple of countries and territories within Russian sphere of influence and control.[62] The System for Transfer of Financial Messages (SPFS) was created also to address U.S. threat of removing key Russian banks from the SWIFT network.[63] Unlike CIPS, SPFS is more of a direct SWIFT substitute given messaging capability. The use of Mir and SFPS is generally constrained to domestic Russian audiences and in countries that are under Russia's geopolitical influence, but are still notable and therefore must be monitored.

BUT DOLLAR IS STILL KING, FOR NOW

Notwithstanding some progress in de-dollarizing separately and jointly, China and Russia are unlikely to meaningful build a global de-dollarized coalition and erode the power of United States. The dollar is still the most appealing currency in the world. One of the most commonly used metrics is the percentage of dollar holdings in foreign

---

[55] Mrugank Bhusari, Maia Nikoladze, "Russia and China: Partners in Dedollarization," The Atlantic Council, February 18, 2022, https://www.atlanticcouncil.org/blogs/econographics/russia-and-china-partners-in-dedollarization/

[56] Bhusari, Nikoladze, "Russia and China: Partners in Dedollarization," The Atlantic Council.

[57] Brendan Murray, "China's Exports to the US Decline While Shipments to Russia Surge," Bloomberg, September 7, 2022, https://www.bloomberg.com/news/newsletters/2022-09-07/supply-chain-latest-china-s-exports-to-us-fall-as-russian-trade-grows.

[58] Lee, "China (Mainland) May Move to Limit Impact of US Financial Weapons," IHS Markit.

[59] Rebecca M. Nelson, Karen M. Sutter, "De-Dollarization Efforts in China and Russia," Congressional Research Service, July 23, 2021, https://crsreports.congress.gov/product/pdf/IF/IF11885.

[60] Payne Lubbers, Sydney Maki, Selcuk Gokoluk, "Russia's Yearslong Quest to Quit Dollar Eases Impact of Sanctions," February 24, 2022, https://www.bloomberg.com/news/articles/2022-02-24/russia-s-years-long-quest-to-quit-dollar-is-blunting-sanctions.

[61] Nelson, Sutter, "De-Dollarization Efforts in China and Russia," Congressional Research Service.

[62] "Russia Enforces MIR Card Adoption in New Countries," Thepaypers.com, May 26, 2022, https://thepaypers.com/cards/russia-enforces-mir-card-adoption-in-new-countries--1256600.

[63] Nelson, Sutter, "De-Dollarization Efforts in China and Russia," Congressional Research Service.

reserves by all central banks. As of 2022, 59 percent of central banks reserves are held in dollars.[64] Though the percentage has declined gradually in the last two decades, the U.S. dollar dwarfs the next currencies in line (21 percent in Euro, six percent in the Japanese Yen, five percent in GBP, and ten percent in other currencies, which includes the RMB). The political economy that underpins the European community is too fragmented, which makes most value holders look to the incumbently dominant U.S. dollar for store of value given its general political (rule of law) and economic attractiveness (open capital account, deep capital markets, independent central bank). China itself is one of the most substantial holders of dollar-denominated assets, as 50 to 60 percent of its foreign exchange reserves are dollar-denominated.[65]

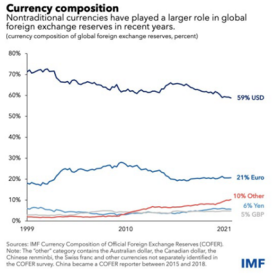


Figure: Currency Composition of Global Foreign Exchange Reserves, 1999-2021 (Source: IMF)

Compared to the U.S. dollar, China's RMB is not traded freely in foreign exchange markets and the inconvertibility makes it unappealing to hold. The Ruble likewise is not widely used, and even in the case of Russia's main export (energy), most transactions are denominated in U.S. dollars. Though Russia intends to shift its energy exports to be denominated in Rubles or other currencies, the main trend would still be dollar-dominated denomination for the immediate future.[66] Most economic actors and institutions would not be switching from dollars to RMB or other currencies overnight. Even when the Euro was released, there was an initial dip in the proportion of dollar-based exchanges, though this rate returned to pre-Euro release equilibrium within a few years.[67] The Global Financial Crisis, an event that should have hurt the dollar's prospects, in fact made the dollar even more of a global safe haven.[68] In the short to medium-term, the dollar's position in the world is unshakable.

---

[64] Serkan Arslanalp, Barry Eichengreen, Chima Simpson-Bell, "Dollar Domicance and the Rise of Nontraditional Reserve Currencies," IMF Blog, https://blogs.imf.org/2022/06/01/dollar-dominance-and-the-rise-of-nontraditional-reserve-currencies/; For those thinking that the 59 percent central banks reserves being held in U.S. dollar is on a declining trend in the last few years, look to the absolute U.S. dollar holdings. Brad Setser from the Council on Foreign Relations rightly pointed out that there are other metrics that correlate with a currency's attractiveness—absolute holdings of dollar reserves being one of them. Even though dollar's share of global reserves fell in recent years, total reserve holdings rose from five percent of global GDP to 15 percent of global GDP. This means the absolute amount of USD holdings actually increased, even though as a share of global reserves it decreased, Twitter, August 29, 2022, https://twitter.com/Brad_Setser/status/1564320134101180416.

[65] Nelson, Sutter, "De-Dollarization Efforts in China and Russia," Congressional Research Service.

[66] Sam Meredith, "Russia to Consider Ditching Dollar-Denominated Oil Contracts if Faced with More U.S. Sanctions," CNBC, June 3, 2021, https://www.cnbc.com/2021/06/03/us-sanctions-may-see-russia-ditch-dollar-denominated-oil-contracts-novak-says.html; Tsvetana Paraskova, "Russia's Grand Plan to Undermine the U.S. Dollar," Oilprice.com, April 4, 2022, https://oilprice.com/Energy/Energy-General/Russias-Grand-Plan-To-Undermine-The-US-Dollar.html; Phil Rosen, "China is Buying Russian Energy with Its Own Currency, Marking the First Commodities Paid for in Yuan Since Western Sanctions Hit Moscow," Markets Insider, April 7, 2022, https://markets.businessinsider.com/news/commodities/dollar-vs-yuan-china-buys-russian-oil-coal-ukraine-sanctions-2022-4.

[67] Eswar Prasad, "Has the Dollar Lost Ground as the Dominant International Currency?" Global Economy and Development at Brookings, September 2019, https://www.brookings.edu/wp-content/uploads/2019/09/DollarInGlobalFinance.final_.9.20.pdf.

[68] Prasad, "Has the Dollar Lost Ground as the Dominant International Currency?" 1.

IV. What's Next?

THE BASE CASE VS. ALTERNATIVE CASE FOR FUTURE GLOBAL FINANCIAL ORDER

The base case of the future of financial statecraft would still be the *status quo*. This would be a continuation of the U.S. dollar serving as the world's reserve currency, and the associated financial infrastructure maintaining the USD's penetration and influence. Barring drastic shift in U.S. financial policy, the United States would continue to be the absorber of last resort and accumulate global savings.[69] As long as the U.S. dollar is the pre-eminent currency, and the United States maintains its unique economic and financial advantages, alternative payment systems like CIPS, eCNY, and SPFS would not be able to mount meaningful challenges. It would be difficult for countries like China and Russia to provide a credible currency alternative to the U.S. dollar. Though, it is a little more likely that China could get more financial institutions to start using CIPS for RMB clearing and settling, and utilize CIPS to help countries like Russia by transacting in RMB. There is a possibility that enough alternative financial rails could coalesce into a critical mass that provides escape valves for sanctioned regimes. Sanctioned entities may be able to trade on alternative payment systems, even though they may be penalized by G7 economies. The level of these transactions might not meaningfully evading the power of U.S. economic and financial sanctions; nevertheless, this base case scenario still requires attention.

Policy considerations also should not stop at the base case. If the PRC leadership makes painful political and economic reforms down the line and actually liberalizes its capital account, the Chinese political economic model could become more attractive, and the RMB might just become a more appealing store of value. This could mean the Chinese and other alternative payment systems and financial rails could over time garner critical mass in adoption. In the event that the PRC thoroughly reforms its political and economic system, it would have had years to fine-tune and perfect its payment systems and financial rails. CIPS and other financial mechanisms and digital innovations could embolden the PRC to contend with mainstream financial plumbing. Foreign financial institutions and firms may be compelled to adopt CIPS clearing and settlement, as they likely would not want to miss out on participating in China's market and alternative systems. In that case, maybe, the PRC and other countries could get to a position of strength to challenge the United States in the global financial order.

In either the base case or the alternative case for future global financial order, there are immediate actions the United States should take.

RECOMMENDED PLANS OF ACTION

Now is the right time to ask some fundamental questions about the role of the U.S. dollar. Does the United States have the political and economic wherewithal to continue to absorb the world's savings? If yes, how should the United States maintain the political and economic institutions that underwrite the dollar's strength? If not, then is the United States willing to make room for a multi-polar financial order? The competition over payment systems may seem like it is about technical offerings, but it really is an outgrowth of a systems-level competition between different political economic leaderships. The United States can best position itself as the center of gravity of the global financial order by:

- **Monitoring the use, growth, and connectivity of these alternative payment rails with the rest of the world.** Though the United States enjoys a prominent position in the global financial system, there is more uncertainty in the outlook for global financial order as policymakers extend their time horizon. There are a couple of factors that policymakers should be monitoring—extent of cross-border trade usage of major currencies (including the USD and RMB), and the quantity and quality of alternative payment arrangements

[69] Michael Pettis, "Changing the Top Global Currency Means Changing the Patterns of Global Trade," Carnegie Endowment for International Peace, April 12, 2022, https://carnegieendowment.org/chinafinancialmarkets/86878.

between adversarial countries (e.g. China, Russia, Iran). At one point, adversarial regimes may just accumulate enough escape valves to partially alleviate the brunt of financial sanctions in the long term. While the United States government need not be overly alarmed about the strength of the U.S.-led financial order, the Treasury Department and other relevant agencies should keep a watchful eye on these developments.

- **Mandating U.S. government annual report on the use of the dollar in the context of global payment systems.** This could either be a new standalone report, or an additional chapter in the report on Macroeconomic and Foreign Exchange Policies of Major Trading Partners of the United States, which is a semiannual assessment that determines whether trading partners manipulated its currency exchange rate with the U.S. dollar.[70] This additional report or chapter should focus on major currencies' positions in global payment systems, which could also track the growth of alternative payment systems and financial rails. It should monitor China's CIPS and Russia's SFPS, but also aggregate all bilateral currency swaps in the world that could work to erode the United States' financial power.

- **Improving U.S. cross-border payments pipelines to make dollar transactions more efficient.** The United States needs to run faster by refining its own payment systems and financial rails. Global cross border transactions are at around $29 trillion now, but could be projected to grow at around $39 trillion by 2022.[71] The United States government and private sector stakeholders should work together to make cross-border payments easier and less costly over time.

- **Developing economic measures to restrict the advancement of alternative payment rails.** There should be pre-determined policy triggers in the event where a financial institution connects to CIPS directly for activities that would help sanctioned entities evade sanctions. Only in cases with reasonable doubt that there are sanctions evasion efforts afoot, should the Treasury department consider levying secondary sanctions on entities that elected to connect directly to the CIPS network. The Department of the Treasury should study the impact of such secondary sanctions prior to levying such tools, given the high likelihood of unintended secondary effects from such measures.

- **Strengthening expertise in analyzing financial developments and statecraft.** Financial statecraft is economic statecraft directed at influencing capital flows. The U.S. government should support institutions and individuals engaged in conducting research on America's and China's financial participation in the world and their respective financial statecraft. For example, the Department of the Treasury, the Federal Reserve Board of Governors, and the Federal Reserve banks should designate cadres of analysts on conducting annual assessments of currency flows in global payment systems.

- **Drafting a long-term strategy document (updated every two to four years) to signal the direction of U.S. financial statecraft and the administration's thinking for the future of the dollar.** The United States government needs a forest-level strategy on managing digital assets and emerging payment systems and rails, which would be crucial to the United States maintaining prominence in international finance. The Treasury report on "The Future of Money and Payments" released in September 2022 pursuant to Executive Order 14067 was a great start, though its discussion of the role of dollar was in the context of payment systems, not on the pros and cons of the dollar maintaining its dominant position.[72]

[70] U.S. Department of the Treasury, "Treasury Releases Report on Macroeconomic and Foreign Exchange Policies of Major Trading Partners of the United States," June 10 2022, https://home.treasury.gov/news/press-releases/jy0813.
[71] "Payments Across Borders: Three Observations on Challenges and Developments," FedPayments Improvement, https://fedpaymentsimprovement.org/news/blog/payments-across-borders-three-observations-on-challenges-and-developments/.
[72] U.S. Department of the Treasury, "The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067," https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf.

- **Engaging proactively in standard setting bodies for digital assets and financial rails.** According to the recently released Comprehensive Framework for Responsible Development of Digital Assets, the United States government is considering policy objectives for a U.S. CBDC system. While it is unclear the United States would be pursuing a digital dollar, the government should be tracking and consistently assessing the impact of licit and illicit digital assets on the strength and integrity of the U.S. financial system. Irrespective of whether the United States plans to create its own CBDC, it should be participating in standard-setting discussion around sovereign national digital currencies. The U.S. government must exchange with other countries and within organizations such as the BIS to ensure China's digital legibility model does not prevail over the U.S.' and select allies and partners' preference for digital privacy.

As an analyst observing U.S.-China economic, technological, and ideological competition, I am cautiously optimistic that the U.S. government is assessing the developmental trajectories of China's and other countries' alternative payment systems. Policy actions including but not limited to those listed above would be necessary to respond to either the base case or the alternative case scenario for future global financial order.

It is an honor to address the Subcommittee on this critical subject. Thank you again for the opportunity.

Chainalysis

Written Testimony of Jonathan Levin
Co-Founder and Chief Strategy Officer
Chainalysis Inc.

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 the National Security Impacts of Their Growth

September 20, 2022

Chairman Himes, Ranking Member Barr, and distinguished members of the Committee. Thank you for inviting me to testify before you today. My name is Jonathan Levin and I am the Co-Founder and Chief Strategy Officer of Chainalysis. Chainalysis, founded in 2014, is the blockchain data platform. Chainalysis has served the cryptocurrency ecosystem for nearly a decade, developing investigative, compliance, and business intelligence solutions and building trust in blockchains.

I am honored to testify before you today on this important topic. I began studying cryptocurrencies ten years ago through my research as an economist at the University of Oxford. I was interested in the way that the internet could create brand new markets and impact developing economies.

In the '90s, many thought the idea that all companies would one day become internet companies was impossible. Now, it simply feels inevitable. We live in an increasingly digital world – in recent research, the Interactive Advertising Bureau found that the internet economy grew seven times faster than the total U.S. economy during the past four years, a sign that more commerce continues to happen online, whether it be through advertising, e-commerce, or other forms.

This transformation has brought citizens of the world closer together in terms of global connectivity, but it has not been accompanied by as many economic opportunities that were promised to individuals. Cryptocurrency technology provides a new way for people to interact and conduct global commerce, providing economic opportunities for people across the world. One day in the near future, all companies will be web3 companies and cryptocurrencies will be fully integrated into their businesses.

Web3 and the crypto rails upon which it is built will serve as the foundation for future e-commerce and it is vital that the U.S. understand the strategic relevance of these payment systems as payment rails shift. Our payment systems will need to be native to the internet in order to compete directly with China and other nations who are already embracing this future.

The United States has built and facilitated the safest and most mature financial system in the world by creating the guardrails upon which individuals and corporations have clear knowledge of property rights, counterparty risks and the cost of transacting. This has been established over decades by deputizing the creation of money through credit and the establishment of many alternative payment instruments to consumers that have ensured greater financial inclusion, lower costs and more options for online payments.

Cryptocurrencies provide entrepreneurs, creators and individuals with technology to create, interact, and transact in ways that are consistent with the U.S. values of individual creativity and economic freedom. This is in stark contrast to the alternative payment systems that are being proposed by China and other authoritarian regimes which may have very low costs but ultimately end in a state of surveillance and a lack of individual freedom. This becomes a geopolitical threat to the United States when these state-controlled digital currencies grow large enough to compete with the U.S. dollar.

The transparent, accessible, frictionless and borderless characteristics of cryptocurrency and web3 technology are the antidote to the goals of countries like China and their adoption of digital currencies: surveillance and total control of economic activity. However, this only happens if the U.S. embraces this technology.

Even in this 'crypto winter', our research shows that adoption of cryptocurrencies continues to grow, especially in emerging markets. As more people put a higher percentage of their net worth into cryptocurrency, they'll want the ability to use cryptocurrency for the full range of transactions they can currently carry out with fiat, such as lending and borrowing, trading assets, and payments. Web3 will enable them to do that with cryptocurrency faster and more easily than they can today.

Let's use mortgage approvals as an example. Today, borrowers need to go through a cumbersome mortgage application process that relies heavily on human judgment — judgment that studies show often reflects human biases and unfairly punishes marginalized communities. In a web3 world, that process becomes faster and fairer.

With the evolution of web3, we have seen new types of products and contracts taking advantage of the composability that blockchain technology affords. Web3 won't just streamline existing financial activity. It will also unlock new use cases in finance that currently aren't possible with traditional assets. We've only begun to scratch the surface of all that web3 can enable, but already we see a variety of different applications, including investing, borrowing, lending, art, entertainment, culture, decentralized autonomous organizations (DAOs), and digital identity.

The recent Biden Administration Executive Order on Ensuring Responsible Development of Digital Assets, which called for U.S. government agencies to come together and develop clear frameworks and policies around cryptocurrencies is an important start to U.S. leadership in this space. We have seen many reports in just the last week coming out of a

number of agencies, including the U.S. Department of Treasury, U.S. Department of Commerce, and U.S. Department of Justice, highlighting the important work they are doing in this space and their plans and recommendations for future coordinated interagency action to promote responsible innovation, reinforce the U.S. role in leadership in the global financial system, mitigate risks associated with cryptocurrency, protect global financial stability, and promote access to safe and affordable financial services. In addition, the recently-passed CHIPS and Science Act establishes a new position within the Office of Science and Technology Policy to advise the President on matters related to blockchain and cryptocurrencies. These are important steps and Congress and this administration should build upon them.

The U.S. must embrace blockchain and web3 technology in order to maintain economic dominance and ensure its national security. We have the opportunity to lead on this front and ensure that future payment systems are built by U.S. companies with U.S. principles in mind, and that these new payment rails, like past payment rails, become the new global standard. If the U.S. does not act quickly, it runs the risk of falling behind adversarial countries like China and Iran, which have already embraced this technology. Lawmakers and regulators should work with industry to implement reasonable regulations that will allow blockchain and web3 to flourish here in the United States. This will help to grow the cryptocurrency industry here, keeping high-paying jobs and economic activity here. Chainalysis, for example, has 850 employees, approximately 500 of whom are here in the U.S.

As with any new technology, cryptocurrency can be used by both good and bad actors. As such, preventing cryptocurrency from being abused by our adversaries is intricately linked to our continued ability to project prosperity around the world and maintain our national security. Embracing this industry will also help to ensure that businesses stay within the U.S.'s regulatory parameters, rather than moving to jurisdictions that do not regulate cryptocurrency businesses or are viewed as "friendlier" regulatory environments. This is critical from a national security perspective. In government investigations into the illicit use of cryptocurrency, it is important that they be able to identify cash out points in regulated countries in order to obtain identifying information about suspects. In a recent report from the U.S. Department of Justice, titled *How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets*, they note "To effectively combat crime involving cryptocurrency and other digital assets, law enforcement must be able to rapidly obtain evidence concerning the crimes." The report specifically cites different record keeping standards and anti-money laundering/countering the financing of terrorism (AML/CFT) standards for cryptocurrency businesses abroad as a challenge that can impede or stall criminal investigations. It is important to government investigations that law enforcement be able to obtain information from cryptocurrency businesses when alternative payment systems like cryptocurrency are exploited by criminals. When these businesses are in unregulated countries, this process becomes much more difficult and is not always possible.

One point I want to make sure I highlight to the members of this Committee, is that the transparency of cryptocurrency blockchains enhances the ability of policymakers and government agencies to detect, disrupt and, ultimately, deter illicit activity. By mapping a single illicit actor to a cryptocurrency wallet address– for example from a payment made to a ransomware group– law enforcement unlocks immediate insight into the network of wallet addresses and services (e.g., exchanges, mixers, etc.) that facilitate the illicit actor. In contrast, in a traditional finance investigation, a similar tip linking an illicit actor to a bank account is just the beginning of a long, extensive process to request and subpoena records that are manually reviewed and reconciled to generate a comparable amount of insight.

In my testimony, I discuss global trends in cryptocurrency, provide background on Chainalysis, outline how blockchain analysis can be leveraged in investigations, and provide an overview of some of the national security threats we see related to cryptocurrency, including from nation-state actors aligned with North Korea, Iran, Russia, and China. I also provide recommendations for improving the government's national security position in relation to cryptocurrency.

Global Trends in Cryptocurrency

Along with the evolution of different use cases in this space, we have seen global adoption of cryptocurrency evolve around the world. Global adoption of cryptocurrency reached its current all-time high in Q2 2021. Since then, adoption has moved in waves – it fell in Q3, which saw crypto price declines, rebounded in Q4 when we saw prices rebound to new all-time highs, and has fallen in each of the last two quarters as we've entered a bear market. Still, it's important to note that global adoption remains well above its pre-bull market 2019 levels. Our data suggests that many of those attracted by rising prices in 2020 and 2021 stuck around, and continue to invest a significant chunk of their assets in cryptocurrencies.

Emerging markets dominate our 2022 Global Crypto Adoption Index, which is designed to measure grassroots adoption of cryptocurrencies. The World Bank categorizes countries into one of four categories based on income levels and overall economic development: high income, upper middle income, lower middle income, and low income. Using that framework, we found that the middle two categories dominate the top of our index. Out of our top 20 ranked countries, the majority are middle or upper middle income countries:

- Middle income: Vietnam, Philippines, Ukraine, India, Pakistan, Nigeria, Morocco, Nepal, Kenya, and Indonesia
- Upper middle income: Brazil, Thailand, Russia, China, Turkey, Argentina, Colombia, and Ecuador
- High income: United States and United Kingdom

Users in lower middle and upper middle income countries often rely on cryptocurrency to send remittances, preserve their savings in times of fiat currency volatility, and fulfill other

financial needs unique to their economies. These countries also tend to lean on Bitcoin and stablecoins more than other countries.

Around the world, not only have we seen cryptocurrencies and digital assets embraced, but many countries are developing their own digital versions of their central bank money. According to the Atlantic Council, 11 countries have launched central bank digital currencies (CBDCs), while another 14 countries (including China) are in the pilot phase of their CBDC project, and another 73 are either developing or researching a CBDC.

Here in the U.S., according to a study conducted by Pew Research, 16% of Americans say they personally have invested in, traded or otherwise used cryptocurrency. According to the recent *Economic Well-Being of U.S. Households in 2021* survey from the Federal Reserve System Board of Governors, while only 3% of people used cryptocurrencies for payments or transfers, 13% of those people who used cryptocurrency for payments or transfers did not have a bank account. This shows how cryptocurrency is already being explored as a means for the underbanked and unbanked to attain greater financial inclusion. Cryptocurrencies are also increasingly used as a fast, low-cost way to send remittances using solutions like the one that Stellar has developed. This rapid and far-reaching expansion of cryptocurrency adoption around the world further demonstrates the importance of U.S. leadership in this space.

Background on Chainalysis

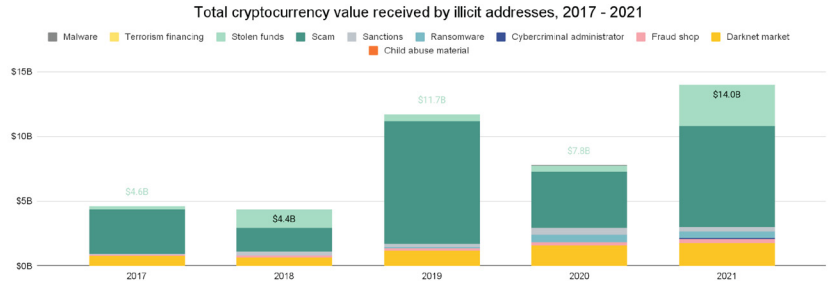
Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. Chainalysis currently has over 850 customers in 70 countries. Our data platform powers investigations, compliance, and risk-management tools that have been used to solve many of the world's most high-profile cyber-crime cases and grow consumer access to cryptocurrency safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of cryptocurrency.

Chainalysis's partnerships with law enforcement and regulators are consistent with our corporate mission: to build trust in blockchains. Fundamentally, we believe in the potential of open, decentralized blockchain networks to drive new efficiencies, reduce barriers for innovators to create new financial and commercial products, encourage innovation, enhance financial inclusion, and unlock competitive forces across financial services and other markets. Our goal is to contribute our data, tools and expertise to drive illicit finance and other risks out of the cryptocurrency ecosystem, enabling the realization of the technology's potential.

Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know Your Transaction), provides cryptocurrency businesses and financial institutions the ability to screen their clients' transactions and ensure that they are

not attempting to interact with illicit services. This transaction monitoring tool provides ongoing insights for cryptocurrency businesses so that they can protect their businesses and clients and meet their regulatory obligations.

Chainalysis also leverages our data to conduct research into the cryptocurrency ecosystem, including the illicit use of cryptocurrency. We publish a number of reports, including our annual Crypto Crime Report. Based on this research, we reported in our 2022 Crypto Crime Report that cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. Top categories include scams, stolen funds, darknet markets, and ransomware. We always caveat these figures, noting that these numbers are the floor, not the ceiling. Our data improves as we learn more about different activities and map out more services, and these numbers will change as we incorporate new information into our data. These numbers also only account for funds derived from "cryptocurrency-native" crime, meaning cybercriminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in cryptocurrency rather than fiat currency.



Despite this large increase in illicit transaction volume, illicit activity as a percentage of total volume has actually fallen since 2019. In 2019, the illicit share was about 3%, in 2020 it was just over 0.5%, and in 2021 it was 0.15%. The reason for this is that cryptocurrency usage is growing faster than ever before, so while cryptocurrency-related crime is definitely increasing, the legitimate use of cryptocurrency is far outpacing its use by illicit actors. This is good news for the cryptocurrency ecosystem, but government and industry must still put in place and implement the appropriate controls to mitigate risks in the system.

How Blockchain Analysis Can Be Leveraged in Investigations

It is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than that of other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone with an internet

connection can look up the entire history of transactions on these blockchains. The ledger shows a string of numbers and letters that transact with another string of numbers and letters. Chainalysis maps these numbers and letters – cryptocurrency addresses – to their real-world services. For example, in Chainalysis products, we are able to see that a given transaction was between a customer at a specific exchange, with a customer at another exchange, between a customer at an exchange and a sanctioned entity, or any other illicit or legitimate service using cryptocurrency. Our data set and investigative tools are invaluable in empowering government and private sector investigators to trace cryptocurrency transactions, identify patterns, and, crucially, see where cryptocurrency users are exchanging cryptocurrency for fiat currency.

Using blockchain analysis tools, law enforcement can trace cryptocurrency addresses to identify the origination and/or cashout points at cryptocurrency exchanges. Law enforcement can serve legal process to these cryptocurrency exchanges, which are required to register as money services businesses (MSBs) here in the United States and collect Know Your Customer (KYC) information from their customers. In response to a subpoena, the exchange will provide law enforcement with any identifying information that it has related to the cryptocurrency transaction(s) in question, such as name, address, and government identification documentation, allowing authorities to further their investigation.

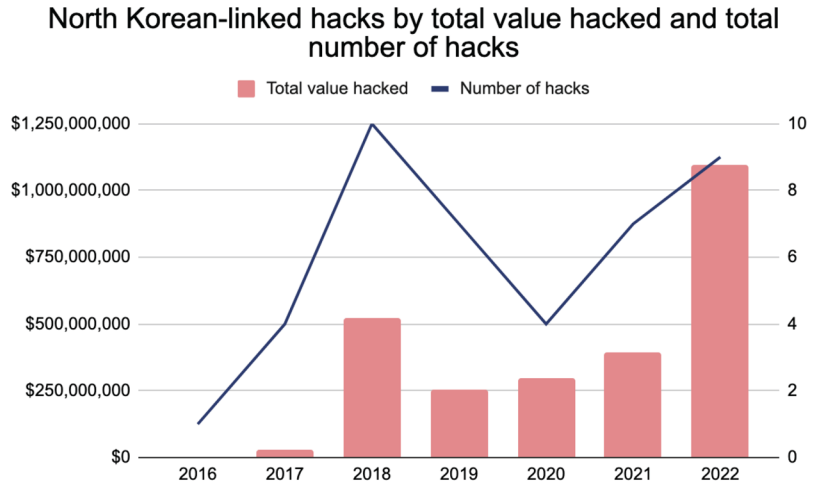
Starting with one cryptocurrency address, from a ransomware payment for example, an investigator can identify not only which address currently holds the funds, but which other addresses are associated with that ransomware actor, as well as which facilitating tools and services enable their attacks, such as access brokers, VPN providers or bulletproof hosting services, and which other groups these actors may be collaborating with. We can tell when members of one group are tied to a new group, whether that is a rebrand, or simply collaboration with another group. This provides invaluable insight into criminal networks and allows government agencies to better prioritize their efforts - and the blockchain trail has time and time again led to outcomes like attribution and even arrest of the perpetrator and asset seizure.

National Security and Cryptocurrency

While, as I have already noted, the overall percentage of illicit activity in cryptocurrency is very small, we do see a number of different adversaries engaged in illicit activities. This is concerning from a national security perspective and should be taken seriously. We must arm our government intelligence and investigative agencies with the right resources and tools to effectively go after these malign foreign actors and mitigate the threat they pose to our national security. I will cover four adversarial countries in my testimony and how they are using cryptocurrencies: North Korea – or the Democratic People's Republic of Korea (DPRK), Iran, Russia, and China.

North Korea

North Korean cybercriminals launched numerous attacks on cryptocurrency platforms over the past few years. Chainalysis estimates that DPRK actors were able to extract nearly $400 million worth of cryptocurrency last year. In 2022, they have already surpassed this number, stealing more than $1 billion from cryptocurrency platforms. Given that North Korea's trade was just $710 million in 2021, the amount of cryptocurrency they are able to steal in these thefts is alarming. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs.



These attacks target investment firms, centralized exchanges, and, increasingly, decentralized exchanges and protocols using phishing lures, code exploits, flash loan attacks, malware, and advanced social engineering to siphon funds out into DPRK-controlled addresses. Once North Korea gains custody of the funds, they begin a careful laundering process to cover up and cash out.

These complex tactics and techniques have led many security researchers to characterize cyber actors for the DPRK is especially true for North Korean hacking group, the "Lazarus Group," which is led by DPRK's primary intelligence agency, the U.S.- and UN-sanctioned Reconnaissance General Bureau. While we will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the Lazarus Group in particular.

Lazarus Group first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime—a strategy that has proven

immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. In March 2022, DPRK was responsible for a theft of more than $600 million from Ronin Network, a sidechain built for the web-based NFT game Axie Infinity. In April 2022, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) updated the SDN List to include cryptocurrency addresses as identifiers for the Lazarus Group. This update confirmed that North Korea had been responsible for the hack of the Ronin bridge attack.

Cryptocurrency's transparency is instrumental to investigating hacks like the one suffered by Axie Infinity. Investigators with the right tools can follow the money to understand and disrupt a cybercrime organization's laundering activities. This would never be possible in traditional financial channels, where money laundering usually involves networks of shell companies and financial institutions in jurisdictions that may not cooperate.

In fact, because of the transparency of cryptocurrency, Chainalysis can tell you exactly what happened in the Ronin hack and how the stolen funds were laundered. The attack began when the Lazarus Group gained access to five of the nine private keys held by transaction validators for Ronin Network's cross-chain bridge. They used this majority to approve two transactions, both withdrawals: one for 173,600 ether (ETH) and the other for 25.5 million USD Coin (USDC). They then initiated their laundering process – and Chainalysis began tracing the funds. The laundering of these funds has leveraged over 12,000 different crypto addresses to-date, which demonstrates the hackers' highly sophisticated laundering capabilities.

There is good news here – law enforcement was able to seize more than $30 million worth of cryptocurrency stolen by these North Korean-linked hackers in this case. This marks the first time ever that cryptocurrency stolen by a North Korean hacking group has been seized, and we're confident it won't be the last.

These seizures would not have been possible without collaboration across the public and private sectors. Much of the funds stolen from Axie Infinity remain unspent in cryptocurrency wallets under the hackers' control. This example underscores the importance of public-private partnerships in promoting our national security.

Iran

Iran's Use of Cryptocurrency in Cross-Border Payments

Iran faces some of the most extensive US sanctions of any country. The Iranian government, including former Iranian President Hasan Ruhani, and several Islamic Revolutionary Guard Corps (IRGC) generals have publicly

endorsed the use of cryptocurrency, including the launch of a central bank digital currency (CBDC), for the explicit purpose of circumventing sanctions.

On August 9, 2022, Iran's Deputy Minister of Industry, Mine & Trade Alireza Peyman-Pak tweeted that Iran had placed its first import order using $10 million worth of cryptocurrency and that, "By the end of September, the use of cryptocurrencies and smart contracts will be widely used in foreign trade with target countries." While Iran's imports using cryptocurrency have not yet been confirmed, two weeks later, on August 29, 2022, Iran's government approved regulations for trading with cryptocurrencies, a move that potentially allows the country to skirt some U.S. financial sanctions imposed over Tehran's nuclear program.

Iran & Cryptocurrency Mining

As one of the world's largest energy producers, Iran has the low-cost electricity needed to mine digital assets like Bitcoin cheaply, providing an injection of monetary value that sanctions can't stop. Our research indicates Iranian Bitcoin mining is well underway at a surprisingly large scale. From 2015 to 2021, we found that Bitcoin mining funneled more than $186 million into Iranian services, most of it within the past year. Iranian state actors are well aware of the opportunity. In 2019, the Iranian government created a licensing regime for cryptocurrency mining. And in March 2021, a think tank tied to the President's office released a report stressing its benefits. The government has actively solicited mining projects to set up shop in the country and take advantage of its low-priced power. They've granted over 1000 licenses to mining operations and according to our data, nearly 17% of funds moving to local Iranian services come from mining entities, compared to just 5% for Middle East-based services overall.

Iranian Ransomware Actors

Iranian ransomware attackers also pose a national security threat. Cybersecurity analysts at Crowdstrike and Microsoft have concluded that many attacks by ransomware strains affiliated with Iran, mostly targeting organizations in the U.S., the E.U., and Israel, leveraging ransomware for financial gain, or objectives of causing disruption or serving as a ruse to conceal espionage activity. Generally speaking, Chainalysis has seen significant growth over the last year in the number of ransomware strains attributed to Iranian cybercriminals in the past year.

Earlier this month, OFAC designated Iran's Ministry of Intelligence and Security (MOIS) and its head, Esmail Khatib, citing their involvement in "cyber espionage and ransomware attacks in support of Iran's political goals." Just last week, the OFAC designated ten individuals and two entities affiliated with Iran's IRGC for their roles in conducting malicious cyber acts, including ransomware activity. According to OFAC, "this IRGC-affiliated group is known to exploit software vulnerabilities in order to carry out their ransomware activities, as well as engage in unauthorized computer access, data exfiltration, and other malicious cyber activities."

In the designation, OFAC listed six cryptocurrency addresses as identifiers for two of the IRGC-affiliated individuals designated for their roles in targeting various networks–including attacks on critical infrastructure–by exploiting well-known vulnerabilities to gain initial access in furtherance of malicious activities, including ransom operations. OFAC specifically cited their role in a February 2021 cyber attack on a New Jersey municipality, a June 2021 system compromise of a U.S.-based children's hospital, and other attacks targeting transportation providers, healthcare practices, emergency service providers, and educational institutions. At the same time, the Federal Bureau of Investigation announced the indictment of three of these Iranian nationals for their roles in a multi-year scheme to compromise the networks of hundreds of companies.

While some Iranian ransomware strains may be used in conventional, financially-motivated attacks by cybercriminals operating in the country, other strains behave more like tools of espionage, extorting negligible amounts of cryptocurrency from victims. Ransomware is a useful cover for strategic denial and deception against enemy states because attacks can be carried out cheaply, and it gives the attacking nation some measure of plausible deniability, as they can always claim the attack was carried out by mere cybercriminals or another nation state.

Earlier this month, a joint Cybersecurity Advisory was released by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, U.S. Cyber Command-Cyber National Mission Force, the Department of the Treasury, the Australian Cyber Security Centre, the Canadian Centre for Cyber Security, and the United Kingdom's National Cyber Security Centre on malicious cyber activity by advanced persistent threat (APT) actors affiliated with the IRGC, highlighting the continued threat to national security these actors pose.

It is important to remember that even ransomware attacks carried out for non-financial reasons leave a trail on the blockchain. For that reason, it's crucial that agencies focused on national security understand how to trace funds using blockchain analysis, as this is the key to identifying the individuals involved in the attacks themselves, the tools they use, and how they launder any funds obtained from victims.

Russia

Russian Use of Cryptocurrencies and CBDCs in Cross-Border Payments

While cryptocurrency is technically banned in Russia, like Iran, Russian plans to use cryptocurrency for cross-border transactions. Just this month, Russian Prime Minister Mikhail Mishustin officially instructed the government to come to a consensus regarding cryptocurrency regulation in Russia by December 19, 2022. He has called for coordinated policies on regulating the issuance and circulation of cryptocurrencies in Russia and asked regulators to finalize regulations for cryptocurrency mining and cross-border transactions in cryptocurrencies. In addition, according to the last monetary policy update from the Bank of

Russia, Russia is also planning to roll out the digital ruble in the next few years, and will begin to connect banks to the digital ruble platform in 2024.

Now-sanctioned oligarch Vladimir Potanin has said the digital ruble and tokens may replace "unregulated" cryptocurrency. He made these comments after Russia's Central Bank gave the local blockchain platform, Atomyze, a license to issue and exchange digital financial assets. Atomyze platform uses blockchain to digitize real assets (like real estate or metals) and convert them into tokens that can be easily exchanged, which allows them to organize the circulation of tokens backed by goods or money on its blockchain platform. These sorts of capabilities may enable Russia's ability to circumvent sanctions to some degree.

Russia-Based High-Risk Exchanges

Interestingly, in spite of the supposed cryptocurrency ban, Russia still ranks #9 on the Chainalysis 2022 Global Crypto Adoption Index, which we released last week. We also know from our research that there are a number of cryptocurrency exchanges based in Moscow City, Russia. Many of these exchanges facilitate significant amounts of money laundering. OFAC has sanctioned several of these exchanges, including Suex, Garantex, and Chatex, which both operated out of the same Moscow City skyscraper: Federation Tower East. While Suex and Chatex have both ceased to operate following their designations by OFAC, Garantex still has existing operations. Nothing is more emblematic of the growth of Russia's crypto crime ecosystem, and of cybercriminals' ability to operate with apparent impunity, than the presence of so many cryptocurrency businesses linked to money laundering in one of the capital city's most notable landmarks.

For some Moscow City cryptocurrency businesses, illicit funds make up as much as 30% or more of all cryptocurrency received, which suggests those businesses may be making a concerted effort to serve a cybercriminal clientele. These sorts of high-risk exchanges are favored by criminal groups, including ransomware groups, as cash out points because they provide an unregulated venue for converting cryptocurrency to fiat without going through the customer due diligence and recordkeeping obligations that exchanges require in parts of the world that regulate cryptocurrency businesses. The use of these sorts of exchanges can stymie investigations in which law enforcement officers seek to find the identity of illicit actors to bring them to justice.

Russian Ransomware actors

As with Iranian ransomware attacks, some Russian ransomware attacks appear to align with geopolitical objectives or employ ransomware as a cover for these goals and Russian ransomware actors are some of the most prolific. Individuals and groups based in Russia — some of whom have been sanctioned by the United States in recent years — account for a disproportionate share of activity in several forms of cryptocurrency-based crime. Chainalysis data suggests roughly 75% of ransomware revenue in 2021 went to strains we can say are highly likely to be affiliated with Russia in some way.

One indication of geopolitical motivations in ransomware attacks is that some of the most pervasive ransomware strains avoid targeting Commonwealth of Independent States (CIS), including Russia, and will fail to encrypt if they detect the operating system is located in a CIS country. Where that fails, ransomware operators have been identified returning decryptors in cases of inadvertent targeting of Russian entities. This suggests at least a tacit tolerance of ransomware activities by the Russian government. In addition, the Russian government has been very reluctant to pursue these groups. In January 2022, Russia arrested 14 alleged members of the REvil ransomware gang, but in June 2022, reports indicated that they intended to drop most of the charges and were "mulling a deal to put the hackers to work for state security services 'in the fight against hackers from Ukraine.'" In other cases, ransomware groups like Evil Corp have been explicitly tied to the Russian government.

In cases where a ransomware strain contains no mechanism to collect payment or allow victims to recover their files, we can be more certain that money isn't the attackers' primary motivation. That's exactly what we saw in a ransomware attack on Ukrainian government agencies by hackers believed to be associated with the Russian government. As the Computer Emergency Response Team of Ukraine (CERT-UA) describes here, a cyber attack occurred on January 13, 2022, disrupting several government agencies' ability to operate. The attack appeared like a ransomware incident, replete with a note and cryptocurrency address provided for payment, that actually belied a malicious wiper known as WhisperGate, that was deleting data at Ukrainian entities. Interestingly, CERT-UA released a report showing that the wiper contains code repurposed from WhiteBlackCrypt, a ransomware strain active in 2021 that was also designed to wipe victims' systems rather than extort them for money.

As the Russian war with Ukraine has continued, there have been an increase in attacks targeting Ukraine that appear aligned with Russian geopolitical goals. An analysis from the Threat Analysis Group (TAG) outlined five different campaigns carried out between April and August 2022 whose activities overlap with a group that the CERT-UA tracks. TAG believes that this group is made up of "former members of the Conti cybercrime group repurposing their techniques to target Ukraine."

We saw a similar situation unfold in 2017, when the Russia-based NotPetya ransomware strain, which contained no viable payment mechanism, targeted several Ukrainian organizations and was also widely judged to be a geopolitically motivated disruption attempt by the Russian military rather than a money-making effort.

Cryptocurrency Fundraising by Pro-Russian Groups

As Russia's war in Ukraine has continued, Russian forces have been accompanied by various militia groups and emboldened by war propaganda. A number of volunteer groups and their supporters have taken to social media to crowdfund military purchases and the spread of disinformation by soliciting cryptocurrency donations. Since the start of the war, Chainalysis has identified 54 such organizations that have collectively received over $3.5

million worth of cryptocurrency, primarily from Bitcoin and Ether donations. Considerable quantities of Tether, Litecoin, and Dogecoin have been sent as well. Roughly half of the donation-collecting accounts have publicly solicited support for militias located in the Donbas region of Ukraine, specifically Donetsk and Luhansk – two territories subject to comprehensive OFAC sanctions as of February 22.

Most of the cryptocurrency donated thus far have been sent to just a few organizations in particular. The cryptocurrency donations sent to these organizations have reportedly been used to support everything from the financing of pro-Russian propaganda sites to the purchase of military items, like drones, weapons, bulletproof vests, communication devices and various other supplies.

Because public blockchains are transparent, we can follow each transfer in these accounts' chains of payments, gleaning insights into pro-Russian activities that would be harder to extract from fiat money investigations. In fact, just last week, OFAC sanctioned Task Force Rusich, one of the above-referenced Russian paramilitary organizations affiliated with Wagner Group, operating in Ukraine — five cryptocurrency addresses we analyzed then were included as identifiers in Rusich's OFAC designation.

Chainalysis continues to work with our partners in the public and private sectors to track these accounts and add new ones as they are identified. We also continue to pay close attention to further indicators of Russian sanctions evasion and cryptocurrency-based money laundering.

China

China and Cryptocurrency

China has historically been one of the largest cryptocurrency markets that Chainalysis studies. China's cryptocurrency industry and user base is one of the most active in the world. China has also historically dominated cryptocurrency mining. At times, China-based mining operations have controlled as much as 65% of Bitcoin's global hashrate — the measurement of how much computing power goes toward mining Bitcoin — which has led to increased liquidity for cryptocurrency services serving China and Asia as a whole, but also concerns that the Chinese Communist Party (CCP) could leverage this control to harm the Bitcoin network. Historical transaction data also suggests that some Chinese cryptocurrency businesses, especially over-the-counter (OTC) brokers, have played an outsized role in facilitating money laundering for those involved in cryptocurrency-based crime.

However, in September 2021, government officials cracked down on cryptocurrency mining and trading, with the global hashrate falling as many Chinese miners paused operations. Interestingly, in spite of the supposed crackdown in China on cryptocurrency trading, China still ranks #10 on Chainalysis 2022 Global Crypto Adoption Index. Our sub-indexes show that China is especially strong in usage of centralized services, placing second overall for purchasing power-adjusted transaction volume at both the overall and retail levels. This is

especially interesting given the Chinese government's crackdown on cryptocurrency activity, which includes a ban on all cryptocurrency trading announced in September 2021. Our data suggests that the ban has either been ineffective or loosely enforced. The industry is generally in agreement that China has dramatically diverted from bitcoin use to altcoins and stablecoins and it's likely that an extensive amount of the activity is conducted on blockchains other than Bitcoin or Ethereum.

China's Digital Yuan

In April 2020, China began testing the digital yuan, becoming one of the first governments to issue a CBDC. CBDCs like the digital yuan (also called the e-CNY) are government-issued, digital versions of a country's national currency. Like most conventional cryptocurrencies, CBDCs would provide greater transparency into how people spend in the aggregate, as the currency's blockchain would act as a permanent, immutable ledger of all transactions. China is rolling out the digital yuan through state-owned banks and digital payment apps like WeChat Pay and AliPay, which are much more widely used in China than their American or European counterparts. Digital yuan trials are ongoing, and many pointed to Beijing's 2022 Winter Olympics as the government's occasion to unveil its new CBDC to the world, as it planned to issue the digital yuan to visiting athletes. According to reports, the digital yuan was used to make 2 million yuan ($315,761) or more of payments a day at the Beijing Winter Olympics, per an official from the Chinese central bank.

According to the Economist, 260 million people and 4.5 million businesses can now use the digital yuan. "Thanks to promotions and handouts, the digital currency has been used in over 260m transactions worth about 83bn yuan ($12bn) since its inception until the end of May, with an average transaction size of about 300 yuan." The digital yuan was designed for retail use so as to be able to rival private payment platforms like Alipay and WeChat Pay. It could improve the government's ability to manage the Chinese economy, but many have expressed concern that the digital yuan will be used as a tool for financial surveillance, and could be a means of subverting U.S. imposed sanctions, as well as the U.S. dollar's position as the world's reserve currency.

Chinese Cyber Actors

Like Iran and Russia, China employs cyber attacks as a geopolitical tool. According to a Bloomberg article, "For more than a decade, Chinese hackers have waged a persistent cyber offensive against Taiwanese government, non-government and corporate targets. Taiwan also happens to be home to some of the electronics, semiconductor and military technology that China desperately wants to get its hands on." These attacks are often used as means to steal sensitive information, such as trade secrets, rather than to demand ransom. However, analysts have also identified instances of ransomware strains affiliated with China, such as ColdLock, carrying out geopolitical attacks on Taiwanese organizations, and Taiwanese authorities have indicated they believe Chinese hackers to be behind attacks on Taiwan's state oil company.

Recommendations

In order to promote U.S. national security, the U.S. can take a number of steps. These include 1) embracing web3 technology and providing regulatory clarity, 2) ensuring U.S. government agencies have the tools, training, and resources they need to conduct and coordinate investigations into the criminal use and national security impacts of cryptocurrency, and 3) improve public-private partnerships. I will detail these recommendations further below.

Embrace web3 technology and provide regulatory guidelines that enable industry to flourish.

The U.S. must embrace this technology and provide clear, workable guardrails for industry participants. While cryptocurrency businesses have been subject to anti-money laundering laws since at least 2013, there are other aspects of the market that still require additional clarification, including direction from Congress. Providing market clarity will support the goals of economic growth and leadership in the U.S. If the U.S. wants to lead in the cryptocurrency sector, we must lead in clear, reasonable cryptocurrency regulation. Clarifying roles around cryptocurrency regulation at the federal level would be a very important step for this market and would help to lend a greater degree of order and enable the industry to grow safely in the U.S.

Ensure adequate funding, resources, and training for government agencies charged with investigating and analyzing the illicit use of cryptocurrency and improve coordination.

As criminals, nation states, and adversaries adopt cryptocurrencies and cryptocurrency technology, governments must keep up with the latest techniques and tactics. Governments that have already embraced blockchain analysis tools have gained invaluable insight and been able to analysis networks and seize millions of dollars in cryptocurrency—further evidence that with the proper tools, investigators can cut off terrorist organizations the funds they need to survive, operate, procure weapons, and carry out attacks. Many government agencies have limited or inconsistent personnel dedicated to investigating and analyzing the illicit use of cryptocurrency. This is often because of a lack of training resources and a lack of funding for new personnel and tools. Allocating appropriate financial and personnel resources to these efforts would ensure that investigators can trace illicit transactions, seize funds, and help bring criminals to justice when criminals exploit cryptocurrency.

In addition to ensuring adequate resourcing, improving coordination among agencies is key. While there are a number of law enforcement agencies that have been building up their blockchain analysis capabilities, these efforts have been siloed and largely uncoordinated. To increase collective impact and achieve large-scale objectives, the U.S. should consider the creation of a National Cryptocurrency Coordination Center. This would house representatives from many U.S. government agencies, working together to investigate and combat the illicit use of cryptocurrencies. The center could also provide training opportunities to the member agencies to raise awareness of what indicators exist in an

investigation to indicate that cryptocurrency might have been exploited, publish resources and reports on trends and how criminal techniques are changing, as well as best practices in investigations, and serve as an information sharing venue private sector liaison efforts.

Improve and augment public-private partnerships

We recommend increasing and improving public-private partnerships in this space. The more information that is shared, the better able we are to combat illicit activities. The U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") Exchange program, which brings together representatives from FinCEN, law enforcement, regulators, and industry members in a voluntary public-private information-sharing partnership is an example that should be looked to and expanded upon wherever possible. These exchanges enable FinCEN to collect and share information in a less formal setting, as well as learn about challenges faced by industry members in their efforts to prevent illicit finance. These sorts of public-private partnerships help to build and improve relationships and sharing mechanisms between the involved parties, with the shared goal of preventing illicit financing and protecting national security. They are also key in an industry that is fast growing and fast evolving – these relationships enable the public sector to better understand what is happening in the private sector and gain key insights that would not be possible without these interactions. Expanding public-private information sharing opportunities among Federal agencies, financial institutions, and private sector experts in banking, national security, and law enforcement is key to improving the U.S. response to illicit financing.

Conclusion

Today, we are living in an increasingly digital world and web3 technology will be foundational to addressing people's desire for fast, frictionless payment systems. These technologies are also some of the best available tools in the toolkit that the United States has to compete with potential national security threats, like ransomware attacks and North Korean hackers. The entrepreneurial dynamism that cryptocurrencies present allows for innovators and builders to create universal access to financial products and re-engineer web2 business models to serve individuals and their data in a way that protects privacy and helps our communities. This technology is consistent with our American values and has the potential to be strategically more important in great power competition over the next few decades. Of course, we understand concerns about risk and that is why we are here today, but at Chainalysis we know that the inherent open nature of this technology can be leveraged to mitigate the risks associated with it. Cryptocurrency's transparency allows for not only the disruption of illicit financing networks, but also the identification, arrest, and prosecution of bad actors. By providing the resources necessary to understand this threat, law enforcement, the intelligence community, and the U.S. government as a whole will be better equipped to mitigate risks and investigate and disrupt national security threats.

Testimony before the U.S. House of Representatives Committee on Financial Services Subcommittee on National Security, International Development and Monetary Policy

"Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth"

September 17, 2022

Dr. Carla Norrlöf

Nonresident Senior Fellow, GeoEconomics Center, Atlantic Council,

Professor of Political Science, University of Toronto

Dear Committee Members, thank you Chairwoman Waters and Ranking Member McHenry and also Subcommittee Chairman Himes and Ranking Member Barr, for inviting me to testify on the important topic of alternative payments system and the national security implications of their growth. I am honored.

My testimony is based on an upcoming report, adapted for this statement, for the Frankfurt Forum organized by the Atlantic Council's GeoEconomics Center and Atlantik-Brücke.[1]

The core point I wish to highlight is that alternative payments systems are growing, with potential national security risks for the United States. The security consequences would be especially concerning if alternative payments were to undercut the dollar's centrality in the international currency system.

Today, the dollar is the only truly *global* currency. Over the medium term, the dollar will continue to be the primary international currency, and is likely to remain dominant over the long term.

Although alternative payments systems do not threaten the dollar's absolute dominance over the foreseeable future, they challenge the extent of the dollar's dominance. We are already witnessing a relative decline in the dollar's status.

---

[1] "Will Economic Statecraft Threaten Western Currency Dominance? Sanctions, Geopolitics, and the Global Monetary Order" I am grateful for the contributions of the Atlantic Council's leadership, Josh Lipsky, the leadership of Atlantik-Brücke, Julia Friedlander, and the staff including Mrugank Bhusari, Sophia Busch, Ananya Kumar, Kathy Butterfield, Katharina Draheim, Franka Ellman, Robin Fehrenbach, Niels Graham, Cate Hansberry, CharlesLichfield, Ole Moehr, and Maia Nikoladze. The views expressed here are my own.

For at least two decades, the international currency system has been unipolar, but after 2017, the system became less unipolar, and in some years came close to becoming a bipolar or multipolar system. Even if relative decline towards other currency majors persists, and ushers in a bipolar or multipolar currency system, an end to the dollar's absolute dominance is nowhere in sight.

Sanctions are likely motivating some countries to diversify away from the dollar, and to devise alternative payments systems to avoid use of the dollar and storing assets in countries where they can be seized. As a countervailing tendency, countries joining US sanction efforts, as well as countries supporting sanction objectives short of imposing sanctions, have geopolitical incentives to diversify into the currencies issued by the sanctions coalition, including dollars. Preliminary analysis of diversification out of Western currencies following the sanctions on Russia in February 2022, suggest modest diversification out of dollars, pound and yen, diversification into Chinese renminbi, other currencies and euros.

If alternative payments systems expand to involve many countries and private users, and cover a wide array of commercial and financial transactions, the dollar will inevitably play a less prominent role than it has in the past, a scenario worth considering.

With the decline in the dollar's importance in the international economy, the economic and geopolitical benefits the United States enjoys as a result of issuing the dollar will also decline. An acute weakening of the dollar's global role will jeopardize the United States' ability to influence, stabilize and enforce international order. The national security ramifications could be significant.

Whenever possible, the United States should work with allies to gain support for major sanction initiatives, as in the case of the recent sanctions against Russia. To mitigate the growth in alternative payments, the United States should avoid sanctions considered to be "unfair" or overly harsh, such as the freezing of the central bank reserves of Afghanistan, which cause alarm about the safety of holding dollar reserves. The United States should exhaust softer, diplomatic, influence attempts before reaching for sanctions, even when maximum campaigns such as blocking a central bank's access to dollar reserves are not being considered. By signaling a commitment to dialogue and cooperative solutions in the overall use of sanctions, "undecided" nations are more likely to remain within the familiar, liquid, dollar system than to sign up to uncertain less liquid alternative payments systems. Lastly, the United States cannot afford to simultaneously adopt a hardline towards foes and allies. The sharpest decline in the polarity of the international currency system coincides with an uptick in sanctions at a time when President Donald J. Trump adopted a tough stance against allies, making them insecure about US security commitments.

69

Will Economic Statecraft Threaten Western Currency Dominance? Sanctions, Geopolitics, and the Global Monetary Order

By Carla Norrlöf

TABLE OF CONTENTS

INTRODUCTION

The security drivers of the Cold War have returned to brace global economic relationships in a more competitive economic environment in which great-power rivals are fully integrated. During the Cold War, geopolitically like-minded states supported one another economically. Geopolitical allies provided each other with assistance ranging from direct aid to currency support to containing economic competition. Economic considerations are once again taking a backseat to security goals. States are moving away from the demands of the market and embracing the demands of geopolitics. Wary of the security consequences of their economic engagement, states are increasingly reluctant to interact commercially and financially with the enemy.

Different from during the Cold War years, great-power rivals today are ambitious participants in the global economic order. Espousing alternative economic arrangements, they seek to upset the prevailing hierarchy in order to gain greater policy flexibility. Preventing Western economic dominance has become more urgent due to their intensified use of economic levers of power to exert geopolitical influence.

The frequency with which economic coercion is practiced is widely anticipated to generate pressures to reduce dependence on the economic instruments and relationships that can be used to inflict harm.

Over the long term, the United States and Europe, therefore, face geo-economic constraints on the extent to which they can wield economic power for geopolitical ends without pushing targeted states, as well as prospective targets, to nurture connections and institutions where geopolitical differences are not an economic liability. Many experts today believe economic coercion is already being overused and that a heavy price awaits the most enthusiastic users. By providing incentives to create alternative systems and privilege other networks, the use of economic power to realize foreign policy objectives undermines the economic basis for exercising economic coercion.

Concerns about geo-economic backlash are particularly acute when it comes to the use of financial sanctions. Owing to their frequency, swiftness, and impact, they have the power to cause severe eco- nomic distress. The number of countries targeted by financial sanctions grew rapidly as the Cold War drew to a close, widely surpassing growth in the use of other tools of economic statecraft such as trade restrictions. However, not until the early twenty-first century did the absolute number of countries subject to financial sanctions exceed the number of countries subject to trade measures.

No country is more closely associated with financial retribution as a response to policy divergence than the United States. The sheer magnitude of countries against which the United States has levied financial sanctions exceeds the number of countries against which any other country levies sanctions in any given year throughout the postwar era. Similar to the system-wide trend, following the end of the Cold War, the number of countries targeted by US financial sanctions grew at a faster pace than the number of countries targeted by US trade controls.

The United States' proclivity for using financial sanctions to exert influence in the international system is, however, not a new phenomenon or even a post-Cold War phenomenon. Since the mid-1970s, more countries have been battered by US financial sanctions than by commercial barriers. Among countries able to apply economic coercion on any significant system-wide scale, European Union countries, as well as Canada, Japan, and Switzerland, also have a greater tendency to impose financial as compared to export and import controls. In common, these countries have extraordinary financial clout, explaining their preference for using financial leverage as a means of influence over other countries. They also issue the world's primary reserve currencies.

Possessing a reserve currency is of great importance for economic statecraft because major currencies, especially dollars, play an outsized role in payments systems and within financial institutions. Financial sanctions by reserve issuers can drastically limit a country's ability to settle trade and financial payments and result in the freezing of large portions of a country's private and official assets. The freezing of official foreign exchange reserves, as in the recent case of the foreign

exchange reserves held by Russia's central bank, is unusual because foreign exchange reserves are supposed to be "safe". If reserve issuing countries can make the safety valve a country has built up for hard times disappear, countries will instead hold currencies issued by countries that have no reason, or lack the capacity, to sanction them, or they will switch to non-currency reserves, unsettling the currency order.

A few days after the start of Russia's invasion of Ukraine on February 24, 2022, Rana Foroohar, associate editor of the *Financial Times*, rang the bell for a post-dollar world, further financial decoupling, and the emergence of a bipolar financial system centered on the US dollar and the Chinese renminbi.[2] The *Financial Times*' chief economics commentator, Martin Wolf, shared Foroohar's vision of a more disorderly currency order, bifurcated into a Western and a Chinese system, accelerating de-globalization.[3] Gita Gopinath, First Deputy Managing Director of the International Monetary Fund (IMF), sees a more fragmented currency system with the sanctions fallout ushering in a multipolar order with alternative currencies used between multiple groups of countries.[4] Credit Suisse banker Zoltan Pozsar foresees the possible closing of an era.[5] He predicts power shifts based on alternative currencies and gold as well as a greater reserve role for other commodities such as oil and wheat. Calling time-out on the existing currency order, he anticipates the coming of Bretton Woods III, making "Our currency, your problem" history, and "Our commodity, your problem" the new future.[6] Under this scenario, the shortage of commodities caused by the war and the demand for secure reserves combine to create inflationary impulses rocking the price stability underpinning the international role of the dollar and the euro.

The relationship between geopolitics and currency hegemony has regrettably been of limited interest to international political economists despite early attention to the significance of geopolitics for currency hierarchy.[7] The question is raised anew with Russia's invasion of Ukraine and the blistering wave of sanctions leveraging the dollar and euro system with the participation of other central banks. This report discusses the geopolitical drivers of transatlantic currency dominance and the currency consequences of making financial sanctions a cornerstone of national security policy. First, the report provides a brief overview of the hierarchy within the global currency order. Second, it considers how military might and security alliances affect currency support. Third, it probes the impact of sanctions on international currency choice and currency polarity. Dollar reserves declined marginally after

---

[2] FOROOHAR, R. (2022): "China, Russia and the race to a post-dollar world," February 27, 2022, Financial Times: London

[3] WOLF, M. (2022): "A New World of Currency Disorder Looms," March 29, 2022, Financial Times: London

[4] WHEATLEY, J., AND C. SMITH (2022): "Russia sanctions threaten to erode dominance of US dollar, says IMF," March 31, 2022, Financial Times: London

[5] POSZAR, Z. (2022): "Money, Commodities, and Bretton Woods III," March 31, 2022, Credit Suisse: New York.

[6] Ibid.

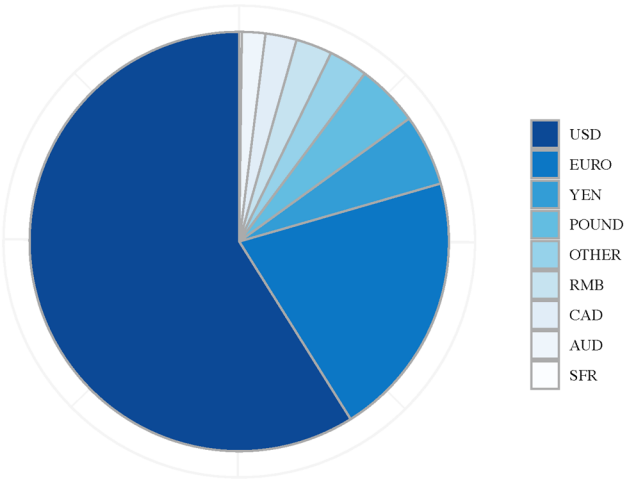
[7] STRANGE, S. (1971): *Sterling and British Policy: A Political Study of an International Currency in Decline*. London: Oxford University Press.

Russia's attack on Ukraine in February 2022 whereas Chinese renminbi reserves grew. The international currency system has however become less unipolar since the launch of the euro in 2002. The sharpest decline in the dollar's reserve centrality coincides with the rise in the number of countries sanctioned by the US since 2017.

1. THE GEOPOLITICS OF TRANSATLANTIC CURRENCY HEGEMONY

The dollar is the *only* global currency and the euro is first amongst the currencies with international reach. At the end of 2021, governments held 59 percent of their reserves in dollars and 21 percent in euros.[8] No other currencies are nearly as popular with governments. The nearest competitor to the dollar and euro, the Japanese yen, accounted for less than 6 percent of governments' currency reserves. Other leading currencies, the British pound, the Chinese renminbi, the Canadian dollar, the Australian dollar, and the Swiss franc, individually account for less than 5 percent of known reserve holdings. Together, all other currencies in the world only add up to 3 percent of reserves held by foreign governments.

Figure 1. Currency Distribution in Official Reserves, 2021



Source: Author's calculations based on IMF (2022).

[8] IMF (2022): "Currency Composition of Official Foreign Exchange Reserves (COFER)," International Monetary Fund: Washington D.C.

There simply is no imminent, or medium-term, threat to the dollar's status as the preeminent global currency, nor to transatlantic dominance of the currency scene. Even under a drastic scenario in which the eurozone project was to fail in the medium term, transatlantic currency dominance would continue. A breakup of the eurozone would imply a return to the eurozone's legacy currencies and restore a prominent role to the German Deutsche mark and to a lesser extent, the French Franc.

Despite this ironclad case for the persistence of transatlantic currency dominance, there is constant speculation about its demise, particularly the demise of dollar hegemony. While an end to the dollar's dominance in the global economy is unrealistic, there are signs of dollar weakening, a trend coinciding with geopolitical rivalry and the intensified use of sanctions. The next section discusses the geopolitical drivers of currency dominance in a longer-term perspective than the current crisis before turning to the constraint sanctions could potentially place on the structure of the global currency order.

Geopolitical strength and security alliances

Economic factors predominantly shape the reserve status of a country's currency. The determinants are the size, sophistication, and growth of the issuing country's economy; asset liquidity; the government's commitment to internal and external price stability; and economic openness. Beyond these determinants, quasi-economic factors also matter, such as the currency's track record, its history as reserve currency, also known as incumbency advantage. Network externalities raise the likelihood of existing and additional users continuing to use the currency because of the advantages of interacting with many users.[9] Dollars, in particular, are traded with great ease, in massive, liquid, and deep markets, resulting in a high degree of stickiness and path dependence. The longer a currency has held a dominant position the more likely it will continue to occupy a central position due to inertia and the pain of switching to an alternative currency. While stable, this equilibrium can be upset. The British pound's loss of international currency supremacy in the 20th century suggests adverse economic and geopolitical trends can combine to knock a currency off its perch. In a research note published in March 2022, Goldman Sachs' Cristina Tessari and Zach Pandl warn about the similarities between the dollar and the pound, notably "a small share of global trade volumes relative to the currency's dominance in international payments, a deteriorating net foreign asset position, and potentially adverse geopolitical developments."[10] However, they see the US economy as more stable than the British economy was, with better prospects to slow inflation, depreciation and the deterioration of the net international investment position.[11]

---

[9] KINDLEBERGER, C. P. (1967): "The Politics of International Money and World Language," Princeton University: Princeton, NJ.
[10] TESSARI, C., AND Z. PANDL (2022): "Global Markets Daily: Lessons for the Dollar from the Fall of the British Pound (Tessari/Pandl)," 30 March 2022, Goldman Sachs: New York.
[11] Ibid.

Geopolitical factors also matter. Since the 1970s, scholars of international political economy have suspected that security considerations shape global currency status.[12] When the euro was formally launched in the early twenty-first century, questions began to surface as to whether it could one day rival the dollar. In a widely read article, economists Menzie Chinn and Jeffrey Frankel provided reasons for "Why the Euro Will Rival the Dollar".[13] Adam Posen retorted, "Why the Euro Will Not Rival the Dollar", arguing geopolitical considerations would interfere with international currency substitution.[14]

Fifty years after the British political economist Susan Strange's seminal work, we still lack good evidence of precisely how and when security variables influence reserve currency status. Theoretically, three broad processes have been identified to raise a currency's attractiveness. First, countries are generally seen as having more confidence in a currency issued by a strong military power.[15] The argument is not one of degree but applies to dominant military powers. Countries infer currency strength from overwhelming military strength.

Second, defense commitments are said to increase a currency's appeal. Countries benefiting from military protection have incentives to hold and transact in their ally's currency as a way of offering economic support. Because economic gains can be used to improve military capability, allies have an interest in bolstering each other economically, particularly the principal power underwriting their security. By using their ally's currency, they enhance the ally's ability to spend on defense, implicitly weakening their common enemy and thereby improving their own security.
The third geopolitical mechanism is a variant of the second. Countries enjoying military protection offer compensation by adopting their security guarantor's currency for reserve purposes. Such a quid-pro-quo is not necessarily motivated by attempts to enhance an ally's economic capability in order to strengthen their own security. Allies are merely trading economic for security guarantees, which they may do voluntarily or be coerced into.

In sum, a strong security position can give rise to enhanced international currency support for several reasons. Beyond economic considerations, countries are understood to be more likely to hold a currency if the issuing country is better able to militarily defend its borders, assets, and institutions against destabilizing attack, or committed to defend other countries' borders, assets, and institutions. To the

---

[12] KELLY, J. (1977): "International Monetary Systems and National Security," in *Economic Issues and National Security*, ed. by K. Knorr, and F. N. Trager. Kansas: University Press of Kansas, 231-59. STRANGE, S. (1971): *Sterling and British Policy: A Political Study of an International Currency in Decline*. London: Oxford University Press.
[13] CHINN, M., AND J. FRANKEL (2008): "Why the Euro Will Rival the Dollar?," *International Finance*, 11, 49-73.
[14] POSEN, A. S. (2008): "Why the Euro will not Rival the Dollar," *International Finance*, 11, 75-100.
[15] BERGSTEN, F. C., *et al.* (1975): "International Economics and International Politics: A Framework Analysis," *International Organization*, 29, 3-36.

extent that these geopolitical considerations incentivize reserve holdings, they give rise to a "security premium."[16] The bonus to the reserve issuing country arises from foreigners' willingness to hold their currency at a higher cost than what is warranted on purely economic grounds. These processes are difficult to substantiate empirically.

Qualitative work has documented the quid pro quo between Germany and the United States during the Cold War, trading military support for currency support.[17] In exchange for stationing 200,000 of its troops in West Germany, the United States asked Berlin for currency support in order to reduce balance of payments pressures under the dollar-exchange standard, resulting in German deposits with the US Federal Reserve. Since American security costs were offset economically by Germany, the bargain is known as the "offset agreement."[18] The best quantitative work has shown how countries are likely to peg to the currency of their ally, in order to confer benefits on friendly countries, boosting their own security.[19] While data on who pegs to which currency is publicly available, we have much more limited knowledge of which country holds which currency and in what proportion. A quantitative proof of how military power or defense alliances or some other geopolitical feature defines reserve currency holdings is, therefore, far more difficult. For instance, Barry Eichengreen, Arnaud Mehl, and Livia Chițu have tried to show that defense pacts enhanced currency support in the late nineteenth and early twentieth centuries, but they leave out crucial economic controls and provide results based on unconventional levels of statistical significance and weak instruments.[20]

To the extent that geopolitics is recognized to influence currency support at all, the security impact is assumed to work through military might and defense commitments. Defense commitments are strong geopolitical ties. Their expected effect on currency support is anticipated to be stronger than other political ties, including other types of alliance commitments. The implicit assumption behind the "defense-for-dollars" argument is that security matters when the stakes are sufficiently high. Alliances, in general, are not considered significant enough to affect international currency choice. Economic considerations are presumed to overwhelm weaker types of alliances, for example, nonaggression pacts, which do not provide enough incentives for pecuniary support. Economic factors are also likely to play a larger role in certain contexts. The salience of defense commitments in international currency choice should not only depend on the level of protection, i.e., the type of alliance commitment, but the level of threat reserve holders experience. For example, some scholars believed the "defense-for-dollars"

---

[16] NORRLOF, C. (2010): *America's Global Advantage: US Hegemony and International Cooperation.* Cambridge: Cambridge University Press.
[17] ZIMMERMANN, H. (2002): *Money and Security: Troops, Monetary Policy, and West Gennany's Relations with the United States and Britain, 1950-1971.* New York: Cambridge University Press.
[18] NORRLOF, C., *et al.* (2020): "Global Monetary Order and the Liberal Order Debate," *International Studies Perspectives*, 21, 109-153.
[19] LI, Q. (2003): "The Effect of Security Alliances on Exchange-Rate Regime Choices," *International Interactions*, 29, 159-193.
[20] EICHENGREEN, B., *et al.* (2019): "Mars or Mercury? The geopolitics of international currency choice*," *Economic Policy*, 34, 315-363.

deal would crumble as defense against the threat of Soviet invasion became less urgent after the Cold War, diminishing support for the dollar, thus weakening its international role.[21]

Countries may also covet other forms of security, for example, freedom from large-scale threats or other third-party conflicts. Even if countries are not covered by a defense guarantee, they benefit from a secure international environment where rivalries are settled amicably, not through war, and where economic exchange is unfettered by conflict. For example, a smaller country like Switzerland may value a stable context for open exchange to a higher degree than France and therefore view the United States as crucial to securing a peaceful context within which economic transactions occur. This would cause Switzerland to support the United States by holding dollar reserves in greater proportion than France in spite of US defense guarantees for France and Switzerland's neutral position.

Standard models of international currency choice do not include defense alliances because even strong political ties of this form are not considered to be of any real significance. The currency a country adopts for reserve currency purposes is presumed to be an economic affair. A country's primary motivation for holding currency reserves is to provide foreign currency to the domestic financial system and to stabilize their currency through interventions in foreign exchange markets during both normal and crisis times. Currency interventions occur toward a specific currency, to maintain a hard peg (a fixed exchange rate), a soft peg, or to loosely align with a foreign currency. The deeper underlying reasons for the currency intervention, and their frequency, vary. The country may be prone to crisis, seek an export-led growth strategy, or chafe under financial inflows unless foreign demand for its currency is neutralized. Countries hold reserves for economic reasons, not to fight wars—or so everyone assumed before Russia's invasion of Ukraine on February 24, 2022.

Geopolitical animosity

Geopolitics, short of military dominance, and alliances may play a larger role than our current understanding of the global currency order suggests. The lesson from the above section is that countries support currency issuers if they are willing and capable of providing some form of security. Countries favor currency issuers that have both the wherewithal to defend their own homeland as well as defending them militarily.

If security reassurances from the currency issuing country contribute to reserve success, destabilizing actions such as sanctions could negatively impact the desire to hold the reserves of the issuing country. Over time, and depending on the viability of alternatives, this could impact a country's reserve currency status. Not all forms of insecurity will reduce countries' willingness to hold a reserve currency. The

[21] CALLEO, D. P. (2009): *Follies of Power: America's Unipolar Fantasy*. New York: Cambridge University Press.

expected effect of insecurity depends on context. For instance, making allies insecure about US defense commitments may cause them to respond with enhanced reserve support if the overall defense-for-money bargain remains intact. Threats to reduce defense commitments may just be teasers to extract greater monetary concessions. If pushed too far, they may have unintended effects. If haggling over security commitments causes allies to believe there is a real prospect of losing protection, any incentive to hold reserves in exchange for protection will be lost. The precise moment when the bargain is likely to collapse is hard to pin down. But at some point, allies will lose confidence in their ability to secure stronger defense commitments, and conclude that the benefits from the security arrangements, which were the precondition for their currency support, are too low to merit ongoing transfers. Threats to revoke security commitments can enhance allies' security and currency contributions but may also backfire to reduce currency support (see figure 3).

If countries are unable to neutralize the effects of insecurity, they may seek to reduce their dependency on the global currency order, either by diversifying currency holdings in the immediate term or by creating alternative payment systems over the long term. The security premium risks becoming a security penalty.

2. THE IN(SECURITY) OF SANCTIONS

Sanctions punish behavior inconsistent with the norms espoused by the sanctioning state. They are threatened in order to deter a wide range of behavior, from human rights abuses to terrorism to war. If the sanctioning state's demands are not met, punitive measures are imposed. In some cases, entire countries are effectively embargoed, but in many cases specific individuals, especially government officials, including facilitating banks, are sanctioned. Even when sanctions are "smart" and "targeted" to hit specific individuals and entities, the consequences for the country where the targeted parties reside can be significant. Because of the human suffering they inflict, sanctions are sometimes described as "economic weapons" and their imposition, therefore, understood to amount to "economic warfare."

For leaders who have no intention of reforming their policies, because their political survival depends on policy continuity, or because they fundamentally disagree about the legitimacy of what they are asked to refrain from doing, aggressive use of sanctions spreads insecurity. Such leaders live in fear that their actions will be met with sanctions and must find ways to weather the storm. They have incentives to fight back, and even undermine the hierarchy and order which make the sanctions possible. There is another part of the equation because security is a double-edged sword, greater insecurity for one country can bring greater security to other countries. Sanctions enhance the security of the sanctioning coalition, and of countries that do not implement sanctions but fundamentally agree with the goal behind the sanctions. Understanding the long-term impact of sanctions on the global

currency order, as well as the immediate impact of the Russia sanctions, requires calculating the net effect of currency actions as the result of both the greater insecurity and security that countries experience when a policy, for instance a sanction, is implemented.

Sanctions and Currency Choice

The currency choices of countries that feel insecure as a result of sanctions will differ from those that experience greater security as a result of sanctions.

Countries that fear sanctions must find coping strategies. One such strategy is to neutralize the impact of the sanctions by building up currency buffers. For example, prior to its invasion of Ukraine, Russia had built up an impressive reserve currency arsenal, to the tune of $630 billion.[22] This strategy effectively reinforces the power of the sanctioning parties since it implies pent-up demand for Western currencies, the main reserve currencies. However, Russia moved a sizeable portion of its foreign exchange reserves offshore, perhaps anticipating sanctions on its central bank. Central bank assets had been frozen before, though in a more limited way. In 2019, for example, the US Treasury Department blocked the assets of Iran's central bank and the National Development Fund used for "terror financing."[23] In 2020, Treasury helped Venezuela's parliament transfer central bank funds from Venezuelan President Nicol.s Maduro to his rival, Juan Guaidó.[24] And in August 2021, Treasury froze assets of Afghanistan's central bank in a bid to make them unavailable to the Taliban.[25] However, these cases do not begin to compare with the size and breadth of the West's Russian asset freeze. On February 24, the day of Russia's invasion of Ukraine, the US and its allies announced sanctions on Russia's most prominent financial institutions, comprising 80% of Russia's bank sector, as well as Russia's central bank.[26] The scope of the coordinated transatlantic freeze on Russia's foreign exchange reserves is unprecedented. Russia responded by requesting ruble denominated energy payments, a logical consequence of not being able to settle in Western currencies.

As a coping strategy, building up a reserve safety valve will no longer be considered a safe strategy by countries who expect profound policy conflict with the United States, and may even scare countries who are uncertain about the degree of policy conflict tolerated by the United States.

---

[22] ZEBALLOS-ROIG, J. (2022): "The US rolls out fresh sanctions meant to block Putin from accessing a $630 billion 'war chest' he could use to prop up a battered economy," February 28, 2022, Business Insider: New York

[23] TREASURY (2019): "Treasury Sanctions Iran's Central Bank and National Development Fund," Washington DC.

[24] AGENCE FRANCE PRESSE (2020): "Venezuela Slams US Over 'Vulgar' Central Bank Funds Seizure," April 17, 2020.

[25] MOHSIN, S. (2021): "U.S. Freezes Nearly $9.5 Billion Afghanistan Central Bank Assets," 17 August, 2021, Bloomberg: New York

[26] NORRLÖF, C. (2022): "The New Economic Containment: Russian Sanctions Signal Commitment to International Order," 18 March, 2022.

Diversification and its limits

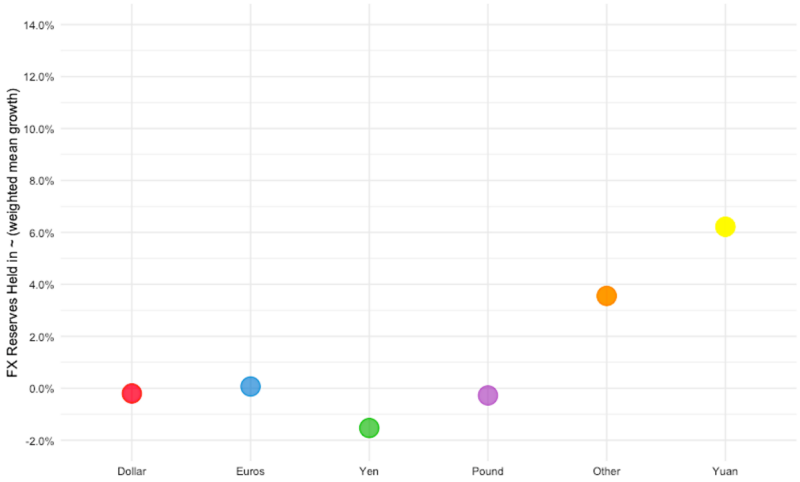
Russia pursued de-dollarization in the years leading up to the war in Ukraine.[27] Diversification partly reflected planned contingencies for relative economic autonomy during the 2022 land grab as well as pre-existing dissatisfaction with US sanctions. Following its first invasion of Ukraine in 2014, and annexation of Crimea, Russia started to diminish dollar-denominated reserves, holding more euros and renminbi instead. Though large in absolute terms, Russia's reserves are a small fraction of global reserves and insufficient to dent the dominance of either the dollar or the euro. A coordinated move with other countries, particularly China, which is the world's single largest reserve holder, could substantially reduce the dollar and the euro's dominance. Even though their rank order will not change over the foreseeable future, increased use of sanctions, and the intensity of the crackdown on Russia, is already causing other potential targets to consider alternatives to the dollar.

Based on a small sample of thirteen countries (see Figure 2), the report finds some diversification away from the dollar between the beginning of the war in February 2022 and June 2022. This modest shift amounts to some twenty basis points. Diversification is primarily occurring into the renminbi and to other minor currencies, and a lesser extent euros. The sample does not include China or Russia, which have geopolitical incentives to continue diversifying out of Western reserve majors, nor does it include Western countries, such as France, Italy, or the United Kingdom, which have incentives to diversify into Western reserve majors in this new geopolitical context. While caution must be exercised when inferring system-wide changes from limited data, these trends suggest sanctions are not causing countries to scramble out of the major Western reserve currencies.

Diversification trends give us some insight into where the wind is blowing, but are insufficient to assess future trends. Even if diversification is much larger than what this sample shows, temporary changes in the composition of official holdings are not sufficient to declare the end of dollar hegemony or the dominance of other Western currencies. However, they could portend larger upcoming changes, which must accompany diversification in order for bigger shifts in the global monetary order to occur.

[27] BHUSARI, M., AND M. NIKOLADZE (2022): "Russia and China: Partners in Dedollarization," February 18. 2022, Atlantic Council: Washington DC.

Figure 1. Reserve Diversification after the Start of the Russian War on Ukraine, 2022



Source: International Monetary Fund.
Notes: Calculations are based on official reserves held by a sample of thirteen countries. in February 2022 and June 2022.

Three things need to change for a multipolar currency order to become entrenched. First, the cross-border commercial and financial exchange for which international currencies are used must increase between countries keen on using alternative currencies. Second, alternative currencies must be easy to access with open economies and payment systems to enable cross-border transactions. Third, the carrying capacity of other reserve issuers must increase. While there is little indication that the biggest reserve contender—China—is capable of absorbing capital inflows consistent with a challenge to the prevailing currency hierarchy, developments on the first and second conditions for an end to the West's dominance are taking place and worth tracking.

Toward currency multipolarity?

International currencies facilitate commerce and investment. They are used to trade goods, services, and assets, including commodities such as oil, and to acquire less widely used currencies.

The oil-for-dollars, or petrodollar, mechanism central to dollar hegemony is being challenged by Russia as well as Middle Eastern and South Asian countries, and is one example of how cross-border exchange could result in greater use of the renminbi and other currencies. In order for developments such as these to pose a

threat to the global currency order, it is not sufficient for currencies to be used to clear and settle economic transactions bilaterally, they must also be used by third parties.

Decades ago, the United States' shaky relations with Middle Eastern states, for example Iraq and Iran, prompted both countries to devise plans to request oil payments in euros. Today, cooperation between Saudi Arabia and China includes provisions for oil debits in renminbi. Both Saudi Arabia and China rightly fear they could become targets of US sanctions. Saudi Arabia's relationship with the United States has been under strain, most recently, due to the murder of Saudi journalist Jamal Khashoggi in 2018 and the kingdom's broader human rights violations. Financial sanctions have already been imposed against China for its human-rights abuses against ethnic minorities in the Xinjiang region. The US has also used other tools of economic statecraft, delisting Chinese firms on US stock exchanges, and preventing Chinese firms from investing in the US, on national security grounds. In 2021, China's crackdown in Hong Kong was widely criticized by US officials short of punishing sanctions.

A 2019 bilateral treaty between China and Russia includes provisions to privilege their respective national currencies to settle trade between them, a step in their plans to de-dollarize.[28] Beyond oil, a number of countries are promoting the use of alternative currencies in trade and finance. For example, India has created a mechanism, a Special Rupee Vostro Account, to encourage settlement in Indian rupees. After crediting the account, customers can either purchase Indian goods, make larger greenfield investments, or purchase Indian government securities.[29] A reintroduction of the Cold War era rupee-ruble mechanism was proposed a month after the Russian invasion of Ukraine, which resulted in Western sanctions that banned Russian banks from processing Indian payments via the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Under this alternative scheme, settlement would occur directly between Russian banks holding rupees in India and Indian banks holding rubles in Russia. Volatility in the ruble's exchange rate, as a result of the war, has, however, put the brakes on the rupee-ruble mechanism.

Bilateral agreements to prioritize the use of national currencies in cross-border exchange, such as the aforementioned ones between China and Russia or between Russia and India, will not increase the international currency role of the respective national currencies. However, if multiple pairs of countries adopt the renminbi in oil invoicing, the dollar's use in oil markets will de facto decline, and therefore also its global appeal.

Moreover, if Russia or Saudi Arabia make oil available to other countries in exchange for renminbi, inter- national use of the renminbi will increase and weaken a major reason for holding dollars, with potentially important consequences. Russia

[28] Ibid.
[29] PTI (2022): "RBI announces measures for international trade settlement in rupees," 11 July, 2022, Deccan Herald: Bangalore

and Saudi Arabia may seem like obvious partners to such an oil-for-renminbi coalition. Competition between them for oil market shares however inhibits collaboration. In 2020, Russia upended a three-year agreement with Saudi Arabia to restrict oil supply aimed at maintaining high prices. Predictably sending oil prices into free fall, the move upset Saudi Arabia.[30]

To displace dollars in the oil market, renminbi invoicing must be actively encouraged over dollar invoicing. Given how many countries settle oil in liquid dollars, restricting the choice for dollar invoicing will initially be unpopular. Caught between a rock and a hard place, Russia will have to choose between alleviating sanctions pressures and plucking dollar customers in the price war with Saudi Arabia.

Initiatives also exist to facilitate purchases in minor currencies, with international currency implications for those currencies. For example, Russia recently ousted Saudi Arabia as the second-largest oil exporter to India, after Iraq.[31] The United Arab Emirates' currency, the dirham, is being promoted for oil settlement between Russia and India. Gazprombank and Rosneft have already started invoicing oil in dirhams.[32] Acquiring dirhams is attractive for Russians seeking to bypass the dollar, promote a more multipolar currency order, and recycle Russian wealth in a sanctions haven. Dubai has become the go-to destination for Russian investors looking to evade sanctions with Russian real estate investment in Dubai doubling in the first half of 2022 as compared to the first half of 2021.[33] Dubai has also emerged as a financial hub for the Middle East, Africa, and South Asia, offering investment opportunities beyond the real estate market, resulting in the Financial Action Task Force (FATF) placing the United Arab Emirates on its "gray list" of countries facilitating dirty money transactions.[34]

An important dimension of understanding the use of alternative currencies in trade and finance are the choices made by the private sector. One indication of a currency's attractiveness is the extent to which it is used to denominate financial assets, for instance, when issuing bonds outside the home country. Data is not yet available to measure the sanctions impact after Russia's February invasion of Ukraine. However, existing data reveals that the dollar has grown significantly in popularity with financial institutions since Russia's 2014 invasion of Ukraine when Russia began gathering support for a new global monetary order. Use of the euro declined. Other private actors increased their international use of dollars in bond issuance. Their use of euros increased to an even greater extent. Monitoring such

---

[30] WARD, A. (2020): "The Saudi Arabia-Russia oil war, explained," March 9, 2020, Vox
[31] VERMA, N. (2022): "Russia becomes India's second biggest oil exporter, trade sources' data show," June 13, 2022, Reuters: London
[32] — (2022): "Exclusive: Russia seeking oil payments from India in dirhams," 18 July, 2022, Reuters: London
[33] TURAK, N. (2022): "Villas by the sea: Rich Russians fleeing sanctions are pumping up Dubai's property sector," 7 July, 2022, CNBC: New York.
[34] KEMP, T., AND N. KURAK (2022): "UAE is placed on money laundering watchdog's 'gray list'," March 5, 2022, CNBC: New York

trends can provide clues about the underlying financial and commercial structure relevant for future international currency trends.

China has taken steps to increase the use of the renminbi for reserve purposes. Since 2016, the renminbi has been included in the IMF's reserve basket of Special Drawing Rights. China began extending bilateral swap lines in 2009 in the wake of the financial crisis. The largest bilateral swap line is with Russia, to the tune of $24 billion. More recently, China has collaborated with the Bank for International Settlements (BIS) to create a Renminbi Liquidity Arrangement (RMBLA) to support contributing central banks in times of crisis. The central banks of Chile, Hong Kong, Indonesia, Malaysia, and Singapore have pledged $2 billion each in renminbi or dollars to the reserve pool which will be housed with the BIS in Basel, Switzerland. Though China's reserve and liquidity provision volumes remain modest, they are likely to grow. These measures are the kinds of steps required for the renminbi to play a role as an intervention currency, for countries to start aligning their currency with the renminbi, and for China to assume lender of last resort functions in times of crisis. The more easily accessible, and liquid, the renminbi becomes, the greater the likelihood it will emerge as an alternative settlement currency.

Significant international currency issuance requires investors and governments to have easy access to the currency at low cost and in high volumes. The Chinese government has been reluctant to embrace full currency convertibility and capital account convertibility for domestic political reasons. It has, how- ever, taken decisive action to create its own clearing and settlement mechanism—China's Cross-Border Interbank Payment System (CIPS)—to promote the use of the renminbi commercially and financially. Similar to the US Clearing House Interbank Payments System (CHIPS), CIPS facilitates transactions, allowing funds to be moved and settled. It is different from SWIFT, both in terms of use and scale, which boasts nearly ten times as many users (around eleven thousand) as CIPS (around one thousand three hundred). Like CHIPS, CIPS relies on SWIFT for financial communication. Eventually, China may devise its own messaging system for complete financial independence in cross-border settlements. The payments initiative plays an important supporting role in China's aspiration to gain financial clout, with more users likely to sign on with time. Similar to SWIFT, the Bank of Russia created a financial messaging system— FMS—to bypass SWIFT after the 2014 Ukraine crisis. Here, the scale is even smaller, comprising only four hundred users.

Lastly, balance of payment constraints impede large-scale currency diversification because no other country is willing or presently capable of absorbing large capital inflows in exchange for liquidity creation. Purchasing assets denominated in alternative currencies from other countries, instead of US dollar denominated assets, implies those countries must be prepared to absorb the trade deficit associated with the capital inflow. In the postwar era, no country, or group of countries, has been willing to run large- scale deficits to support currency dominance on the scale that the United States has tolerated current account disequilibrium.

Figure 2 above showed minimal diversification away from the US dollar, the euro and the British pound, and some diversification away from the Japanese yen,

between February 2022 when Russia invaded Ukraine and the summer of 2022. In a longer term perspective, countries have diversified away from the US dollar, particularly after a credible alternative to the dollar became available following the euro's launch in 2002. The trend was interrupted with the fallout from the 2008 financial crisis which resulted in the sovereign debt crisis of 2009 in euro-zone countries. Since 2009 and up until 2017, the dollar gained ground vis-a-vis the euro. These trends can be seen in Figure 3 below, which show the number of countries sanctioned by the United States every year between 2002 and 2019 along with two different measures of currency polarity.

Polarity is usually used to describe the distribution of military power in the international system but can also be applied to analyze the distribution of currency power in the international system. A pole is a great power with extraordinary capability within the substantive area under consideration. For example when the "unipolar moment" was declared at the end of the Cold War, Russia, Great Britain, Japan, and France were still considered to be great powers, though not of the same caliber as the United States.[35] The military power gap between them was far too large for them to be considered similar types of great powers.[36]

Figure 2 above showed minimal diversification away from the US dollar, the euro and the British pound, and some diversification away from the Japanese yen, between February 2022 when Russia invaded Ukraine and the summer of 2022. In a longer term perspective, countries have diversified away from the US dollar, particularly after a credible alternative to the dollar became available following the euro's launch in 2002. The trend was interrupted with the fallout from the 2008 financial crisis which resulted in the sovereign debt crisis of 2009 in euro-zone countries. Since 2009 and up until 2017, the dollar gained ground vis-a-vis the euro. These trends can be seen in Figure 3 below, which show the number of countries sanctioned by the United States every year between 2002 and 2019 along with two different measures of currency polarity.

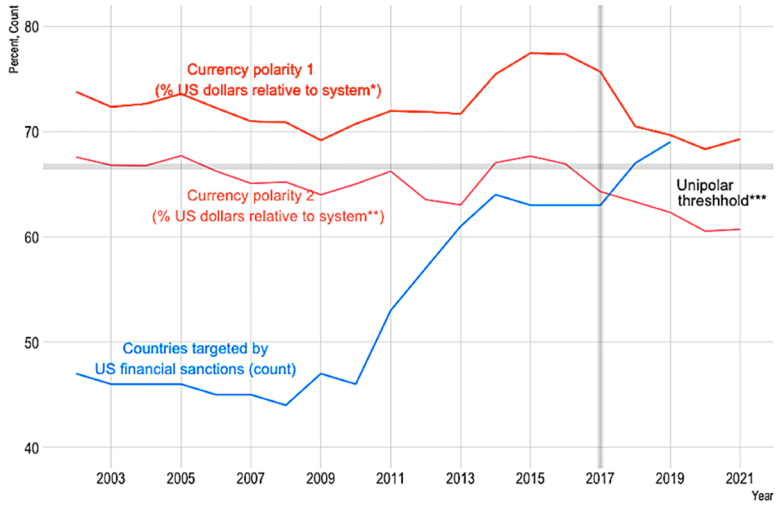
Some method is needed to determine how much relative power is needed to qualify as a great power. The first, and more accurate, measure of currency polarity assumes the system of great power reserve issuers should only comprise countries issuing core reserve majors—the US dollar, the euro and the Japanese yen.[37] Core majors are reserve currencies which account for at least 5 percent of foreign exchange reserves.[38] The second measure of polarity assumes the system of great power reserve issuers includes any country issuing a reserve major, regardless of how widely their currency is used for reserve purposes. In this measure, small issuers accounting for less than 1 percent of foreign exchange reserves, such as Switzerland, are also part of the system of great power reserve issuers. Regardless of

---

[35] KRAUTHAMMER, C. (1990): "The Unipolar Moment," *Foreign Affairs*, 70, 23-33.
[36] WOHLFORTH, W. C. (1999): "The Stability of a Unipolar World," *International Security*, 24, 5-41.
[37] Cohesive entities such as the euro-zone countries are also included, but not the category "other" issuers since it includes disparate countries and not a cohesive group of countries.
[38] To be more precise, more than 5 percent of all allocated reserves are held in these currencies. Allocated reserves are foreign exchange reserves for which the currency breakdown is known.

how the system of great power reserve issuers is defined, polarity is quantified as the share of US dollar reserves relative to the system.

Figure 3. Currency Polarity and Financial Sanctions



Source: Author's calculations based on International Monetary Fund.
Notes: The first measure of polarity is the share of reserves held in US dollars relative to the reserves held in the currencies of the core major issuers (the USA, Euro-zone and Japan) and in US dollars. The second measure of polarity is the share of reserves held in US dollars relative to the reserves held in all reserve majors including US dollars. *Unipolar threshold represents the minimum US dollar share of the system in order for the US dollar to be considered a unipolar currency, accounting for two-thirds of the system's reserves.

How much "more powerful" must a great power currency issuer be in order to qualify as a unipole? Figure 3 defines unipolarity as a system where one great power's reserve issuance is twice as large as the reserves issued by the other great powers in the system. This definition of unipolarity applies to both measures of polarity, and represents a clear-cut case of unipolarity. The cut off point is conservative. A case for unipolarity could be made at lower levels of power disparity between a leading provider of reserves and providers of other currency majors in the system. When the reserve issuance of one great power is twice as large as the amount of reserves issued by other great powers in the system, the unipole issues two-thirds of all the reserves in the system. Figure 3 therefore draws a line, the unipolar threshold, at the point where the international currency system is unipolar, with reserves in US dollars accounting for at least two-thirds of all reserves in the

system. Below this floor, the international currency system is either bipolar or multipolar.

As shown in Figure 3, it is possible that factors quite apart from financial sanctions may be driving the decline in dollar unipolarity. When the number of countries targeted by US sanctions stayed constant be- fore 2010, dollar unipolarity declined on both measures. As the number of countries facing US sanctions increased as of 2010, the first, more accurate, measure of dollar polarity, increased up until 2015. It also bears underlining that if sanctions matter for currency polarity, it is not just the number of countries that is of relevance. After Russia's first invasion of Ukraine in 2014, the number of countries hit by US financial sanctions stayed the same, but dollar unipolarity decreased on the second measure, which accounts for a greater number of currency majors when evaluating polarity. The implication is that smaller reserve issuers grew in importance during this time. When the number of countries met by US financial sanctions rose sharply as of 2017, and a President threatening to revoke alliance commitments was elected, dollar unipolarity declined on both measures, with the first measure reaching its lowest point in two decades and headed below the unipolar threshold.

CONCLUSION

A more fraught international environment is having negative repercussions on countries' willingness to remain economically interdependent. Geopolitical rivalry has rejigged the neat separation between economic and security affairs. Countries still seek gains from open economic exchange, but are wary of their national security ramifications. Reminiscent of the Cold War era, governments are paying more attention to ensuring countries they support economically are countries they support geopolitically. In this new context, international economic relationships risk becoming subordinated to geopolitical relationships. Several analysts believe that the international role of the dollar was in part a function of the United States' geopolitical role, particularly during the Cold War years. When the threat of the Soviet Union dissipated, some believed an important incentive to hold dollars beyond its economic appeal, was removed. The euro's launch in 2002, and the creation of a viable reserve alternative, made it possible to reassess reserve holdings in dollars. Fears about dollar collapse started to surface.

Today, these qualms have returned with a vengeance. This time, the worry is not that allies no longer have security reasons to support the dollar. Instead, states dissatisfied with the current international order are possibly cultivating economic alternatives to the Western-led economic order. Endowed with the world's largest financial institutions and the world's first currencies, Western countries, particularly the United States and Europe, are increasingly using financial sanctions as a way of policing inter- national order. Countries with which they have fundamental

disagreements will reconsider pursuing policies that may be met with heavy sanctions and feel less secure about using Western currencies. So far, countries have not diversified away from Western currencies to any great extent in response to Russia's 2022 invasion of Ukraine, but developments are underway to bypass the dollar and the euro. Greater use of Chinese renminbi, and more minor currencies, will not put an end to the Western centric currency system, but if unchecked, it could accelerate the slide away from the dollar's unipolarity, reinforcing a longer-term trend. Dollar hegemony has however bounced back from previous downward cycles. The large lead to competitor currencies suggests this time is unlikely to be different as long as the US maintains a strong economy, open markets, and ties to allies.

Annex

Glossary

BIS	Bank for International Settlements
CHIPS	Clearing House Interbank Payments System
CIPS	Cross-Border Interbank Payment System
RMBLA	Renminbi Liquidity Arrangement
SWIFT	Society for Worldwide Interbank Financial Telecommunication

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.

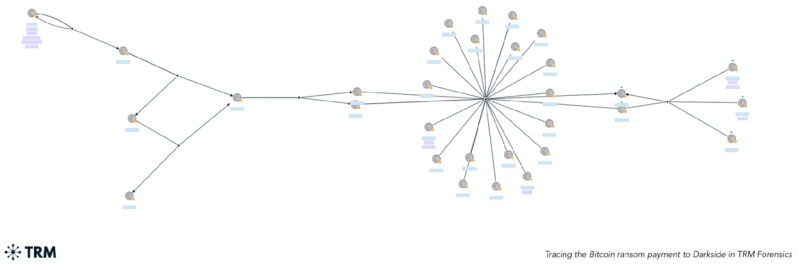
Because blockchains provide an immutable audit trail of every transaction, understanding the ultimate source and destination of funds, particularly across jurisdictions, is substantially easier, faster, and more reliable compared to tracing funds through traditional financing mechanisms. Blockchain intelligence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

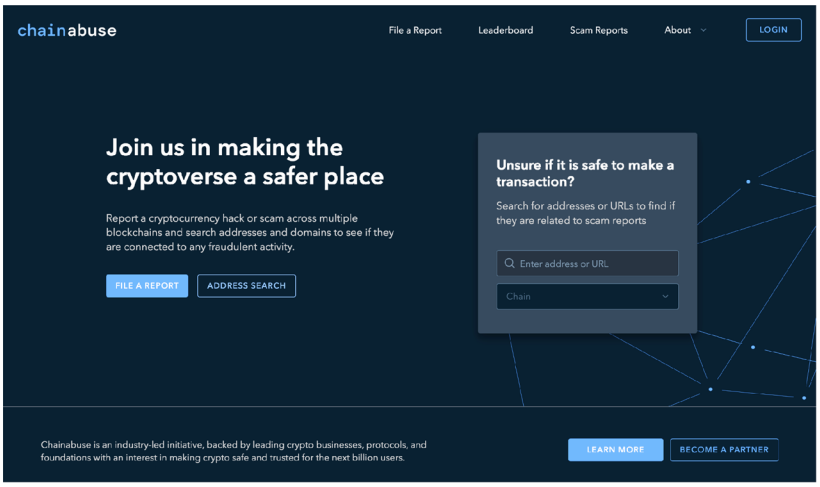
Public

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.

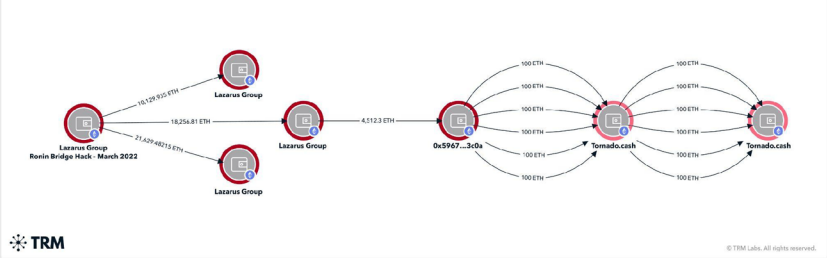
Blockchain-based “digital passports” could allow individuals and entities to store proof of KYC verification directly on the blockchain, a “win-win” for all parties—customers, institutions, and government—involved in transactions. Customers would seamlessly access financial services and minimize the 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.

Image source: Stock Illustration ID: 1896598609 by KanawatTH (n.d.). Retrieved from: https://www.shutterstock.com/image-illustration/bitcoin-blockchain-crypto-currency-digital-encryption-1896598609

Author

Scott Dueweke

Global Fellow

Black Swans and Green Fields:

Exploring the Threat and Opportunity of the Alternative Payments Ecosystem to the West

August 2022

TABLE OF CONTENTS

In 2009, Satoshi Nakamoto published a white paper describing a digital cryptocurrency called Bitcoin. Fast-forward to a post-pandemic 2022, and the stability of the global financial ecosystem is being forced to adapt to what has followed, as a range of virtual currencies (VCs) gain global relevance. The West's financial hegemony is being threatened by both centralized virtual currencies (especially Chinese and Russian) and decentralized virtual currencies (e.g., Bitcoin and other cryptocurrencies) which have exploded in popularity and viability.

These new financial systems provide a growing, increasingly viable, and capable set of interconnected non-bank financial channels representing an Alternative Payments Ecosystem (APE). These systems may or may never touch the legacy financial system consisting of banks and other traditional financial institutions bound together within and across global borders through messaging networks such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) or the Automated Clearing House (ACH). Any discussion of the APE immediately turns to Bitcoin and other cryptocurrencies, and it's understandable why, as the financial world seemed to change when Satoshi Nakamoto's 2009 paper was released. Yet the APE extends far beyond these blockchain-based systems. The APE story does not begin there nor is it the only story being written.

But let's first consider what Virtual Currencies (VCs) are: digital representations of value, issued by private developers (for now, at least), and denominated in their own unit of account. VCs can be obtained, stored, accessed, transferred, and transacted digitally, and they can be used for whatever purpose the transacting parties have agreed to use them. The concept of VCs covers a wider array of "currencies," ranging from simple IOUs of issuers (e.g., vouchers, loyalty points) and VCs backed by tangible assets (e.g., precious metals) to a national "fiat" currency and even cryptocurrencies. They are used for transmitting value from one party to another without using the traditional financial system for that payment or transfer. Systems like Tether or WebMoney may be transferring U.S. dollars (USD), Russian rubles, or gold, yet that transfer is often occurring outside of the banking payment processing world. These systems are centralized virtual currencies (CVCs) —centralized because an entity runs them—or decentralized virtual currencies (DVCs) like Bitcoin and other cryptocurrencies which run themselves. These CVCs and DVCs often fall outside of any reporting requirements to western financial regulators.

Despite the popular and policymaking focus on cryptocurrencies, the largest systems found on the APE are not DVCs. By orders of magnitude, the largest are actually China's CVCs which are virtual currency, mobile, or social media payment system hybrids. No bank controls these systems, but rather large corporations. Combined, two major companies – Tencent and Ant Group – processed 294.6 trillion yuan (US$45.6 trillion) in 827.3 billion transactions in 2020, representing significant growth over 2019 (PYMNTS, 2021).

Image source: Stock Photo ID 1039844908 by stockphoto-graf (n.d.). Retrieved from: https://www.shutterstock.com/image-photo/crypto-currency-coin-panorama-set-collection-1039844908

Fungibility

The connective tissues for the APE are the Virtual Currency Exchangers (VCEs) that allow the trade and exchange, often unfettered, of all of the previously mentioned VC examples. CVCs, traditional payment systems, DVCs, and even game or esports credits can be used to purchase Bitcoins and other cryptocurrencies on the U.S.-based Paxful.com and other Peer-to-Peer (P2P) and Over-the-Counter (OTC) exchange sites. Western Union and other remittance systems can be exchanged for VCs on dozens, if not hundreds of VCEs. Most of the VCEs based in the West, such as the U.S.-based Coinbase, expend great effort and expense to meet all the requirements of being a properly certified Money Service Business (MSB). Those outside of the direct reach of relevant regulators are not always so willing to expend the resources and effort to comply with the applicable U.S. Patriot Act and Bank Secrecy Act (BSA) requirements.

MSBs are heavily regulated in the United States, both by federal law and by statutes in 49 of the 50 states. VCEs are considered MSBs if they offer financial services related to cryptocurrencies such as the exchange of CVCs, stored value cards, or the conversion of fiat currencies into digital forms—the exchange or dealing of currency or money transmission. One of the primary reasons for this tight regulatory management of MSBs is tax collection. Despite the IRS' repeated attempts to thwart cryptocurrency's use in tax evasion, which IRS Commissioner Charles Rettig continues to attribute part of the growing US$1 trillion tax gap, the IRS is in desperate need of assistance in the fight against tax evasion (Rappeport, 2021).

The cost of compliance and the lucrative opportunities provided by catering to those who want to be as anonymous as possible have resulted in dozens, even hundreds, of VCEs around the world who intentionally avoid globally accepted Know Your Customer (KYC) standards to combat financial crime. The rise in cryptocurrency use has brought many examples of these exchanges. In 2014, Mt. Gox was the first well-known VCE, and also the first VCE to implode through mismanagement, fraud, and criminality; its failure cost those who entrusted it with their VCs over US$2 billion in stolen Bitcoin by today's valuations (Redman, 2022).

With the rise of the Dark Web came illicit virtual currencies. These did not start with Bitcoin, but rather, well before the first cryptocurrency, there were illicit payment systems serving the drug trade and other illegal enterprises online. Liberty Reserve, a CVC created in 2006, had over one million users when its offices in Costa Rica shut down in 2013 in the first multi-national law enforcement action focused on virtual currency. Over US$8 billion had flowed through Liberty Reserve during its 7-year run (U.S. Department of Justice, 2016). There were other services active on the Dark Web as well in the pre-Bitcoin dark ages, most of them CVCs backed by precious metals (the grandparents to the stablecoins of today) such as CGOLD and Pecunix. E-Gold was the best known of these, and it operated until 2009 when it was forced by law enforcement to shut down due to charges of money laundering. The Silk Road marketplace, selling drugs and weapons and more on the dark web, helped to revolutionize all of this illicit use and propelled Bitcoin to be the lifeblood of the Dark Web. Well over US$1 billion of Bitcoin was used in those transactions on Silk Road (Hern, 2020).

The commonality among these examples is that all of these systems relied on their ability to exchange fiat money into digital "cash." Once converted, they could often be used and traded for one another with impunity.

Before eCash and then Bitcoin, it seemed that no one was watching or that law enforcement simply did not care as there were few direct victims of this illicit dark economy. That has changed, however, and today, there are hundreds of cryptocurrencies, CVCs, stored value cards, Mobile Payment Services (MPS), e-vouchers, and more that are traded on hundreds of exchanges. Some even have their own blockchain networks, such as Binance Coin (BNB). Stablecoins and other asset-based coins backed by fiat currencies (such as Tether which uses the U.S. dollar as its stable base) are gaining in acceptance and popularity quickly, even amongst criminals and terrorists; the same purported stability that is attractive to the average investor is attractive to these bad actors. In contrast to ordinary cryptocurrencies, because these are said to be pegged to the value of reserved fiat currencies, these coins have a lower level of volatility. Some stablecoins are following the path carved out by CGOLD and Pecunix, such as the precious metal-backed coin, ZenGold.

Types of Exchanges

1. Decentralized simply refers to the process of being free from central authoritative control and applies primarily to cryptocurrencies. These decentralized exchanges feature:

- No identity verification — KYC/AML
- Non-custodial payments (payments are never in custody of a third party) — P2P [Peer-2-Peer]
- No fiat support
- Examples such as BTCPayServer, Blockonomics, MyCryptoCheckout fall in this category.

2. Centralized exchanges are run by an entity, usually a company that manages the exchange of funds and often provides a wallet for consumer use. These are all categorized as centralized processors as they have access to users' funds in some form or another. They may include the presence of third-party services where an investment vehicle holds the customer's funds or, in more primitive (and often illegal systems), they can simply be held by one party:

- These may be cryptocurrency only, such as Coinbase, BitPay, Coinpayments, Coingate, or Binance
- CVCs such as QIWI or Perfect Money - or a hybrid such as WebMoney.

KYC is the key to differentiating the basic legitimacy and legality of these systems. Those VCEs that dutifully meet regulatory and Financial Action Task Force (FATF) guidelines in knowing with whom they are transacting are starkly different than those who make it their business not to know. As of June 2021, FATF reported that only 58 out of 128 reporting jurisdictions implemented revised standards (FATF, 2021) and recommended that VCEs (FATF and the U.S. Financial Crimes Enforcement Network [FinCEN] refer to them as Virtual Asset Service Providers [VASPs] although there is no accepted standardization) discontinue connections with companies that operate in jurisdictions where the Travel Rule recommendation has not been implemented. However, as FATF recommendations are not laws or regulations, they are not legally binding. Following a recent survey, just 11% of VASPs (Notabene, 2022) have chosen to stop transferring funds to other brokers in countries which have not yet implemented a version of this law.

Cryptocurrency kiosks or automated teller machines (ATMs) are an extension of the VCE model, allowing a person to exchange VCs and fiat currencies. CVC examples of this are QIWI and WebMoney kiosks that are common in the Russian-speaking world. Cryptocurrency ATMs are found in most cities around the world, usually enabling only the buying of crypto, but with some allowing a bi-directional functionality to also sell cryptocurrencies through the machine. Apart from traditional ATMs, crypto-ATMs have no connection to a bank account. Instead, they are directly connected to the crypto exchanges.

Alternative Payments as a Criminal Backbone

Today, we are seeing the largest thefts of cryptocurrencies occurring in the hacking of VCEs, like Bitfinex. In February 2022, the DOJ announced the arrest of two individuals—not in Malta or Panama, but in Manhattan—for an alleged conspiracy to launder cryptocurrency that was stolen during the 2016 hack of the Bitfinex virtual currency exchange; the loss is presently valued at approximately US$4.5 billion (U.S. Department of Justice, 2022). When calculated in 2017, it was estimated that 5% of all Bitcoin ever issued had been stolen from exchanges which hosted their customer's wallets (Roberts & Rapp, 2017). Many of these thefts (and more recently, with the hacking of smart contracts) are being perpetrated by North Korea.

Cryptocurrency can be used to purchase the tools to penetrate bank's defenses, as well as ransomware as a service (RaaS) from the "consumer"-facing Dark Web sites.

But what are smart contracts? Think of them as a way to automate specific functions or business processes so all parties are informed at once. They are particularly well-suited for use in cryptocurrency transactions. The most recent example was carried out, according to the U.S. Treasury, by the North Korean hackers known as the Lazarus Group, which stole US$625 million in cryptocurrency from the Ronin network (the blockchain backing the Axie Infinity play-to-earn crypto game) (Sharma, 2022). In April, the U.S. Treasury Department sanctioned the wallet address that received the stolen funds and attributed the hack to the Lazarus Group. The weak spot targeted by the hackers was the smart contract that acted as the "bridge" that allowed users to transfer funds between other blockchains and Axie Infinity. These flagged wallet addresses currently contain over US$445 million and sent almost US$10 million to another wallet as of May 2022. North Korea's crypto-haul so far this year is estimated to be about US$1billion, offering a method to evade sanctions (Sharma, 2022).

But it's not just the VCEs that criminals are attacking. Bank, payment processors, retailer and other members of the traditional financial sector possess an array of Personally Identifiable Information (PII) that can be combined with other hacked or stolen information and credentials to enable access to cryptocurrency wallets, bank accounts, and access to loan applications. Dark Web sites allow criminals to mix and match these identity elements to effectively monetize (Kellerman & McElroy, 2021). Cryptocurrency can be used to purchase the tools to penetrate bank's defenses, as well as ransomware as a service (RaaS) from the "consumer"-facing Dark

Web sites. The Criminal-to-Criminal (C2C) transactions are more likely to use CVCs to avoid the tracking inherent in blockchain-based cryptocurrencies. These RaaS variants include ingenious business approaches including the use of affiliate programs to expand the reach of these criminal systems, while expanding their revenue model by taking a portion of the revenue generated by ransom payments for all the attacks made by their RaaS-enabled partners (Kellerman & McElroy, 2021). These payments use Bitcoin or, increasingly, anonymity-enhanced systems (AES) like Monero which avoid the public blockchain and shroud their users from identification.

What is Driving the Use of Alternative Payment Systems?

Major drivers of this revolution of alternative payment systems are not easily apparent in the Western world. We think of the speculative aspects of Bitcoin and other cryptocurrencies, of hackers and ransomware, of convenience. Yet, there is a much larger energy that is driving this change: the direct correlation between financial exclusion and poverty. The lack of access to banking or other financial services constrains the opportunities of over 700 million people, accounting for nearly 73% of all the world's poorest people (IFAD, 2015). Among the financially excluded are migrant workers and their families. These populations send remittance payments to their home countries, providing a significant, steady flow of approximately US$500 billion to these economies (IFAD, 2015). These populations also have no access to financial products like insurance, loans or mortgages. This breeds poverty, and the traditional banking system has done little to include them. In places like Somalia, they have done the opposite, cutting often desperately poor and war-weary people off from the lifeline of remittances from diaspora. Through a process called "de-risking" banks make profit-based decisions to close the accounts for remittance companies like the Somalia-based Dahabshiil, although they are thinly veiled as security or risk decisions. In the Middle East and Africa, 50% of the population is unbanked or underbanked, with South and Central America nearing 38%, Eastern Europe at 33% and Asia Pacific at 24% (Ventura, 2021).

Traditional bank-centric financial systems are under siege as the ground beneath them shifts amid the awaking of the unbanked and underbanked, as well as the burgeoning global middle class. Frequent use of financial sanctions has contributed to this shift as Chinese and Russian new payment systems bypass SWIFT and other western-dominated financial backbones. No longer the domain of FINTECH startups, nor just limited to cryptocurrencies, nation states are playing the "Great Game" on new terrain.

In Kenya, mobile money provider M-Pesa has shown the power of new payment systems to transform economies for the better. This mobile money transfer platform is the great experiment in low-tech FINTECH that has transformed Kenya's economy, and is impacting the rest of East Africa, through connecting simple SMS-based phone communications into their own regional SWIFT network. Beginning with its 2007 launch by Vodafone and Kenya-based telco Safaricom, M-Pesa recently hit the 50 million active users mark in Africa, the largest fintech platform on the continent (O'Gardy, 2021).

M-Pesa allows its customers to instantly send money to each other. For many this was their first and often only access to financial services propelling M-Pesa's fast growth and adoption across the country. Its growth has accelerated financial inclusion across the continent. In Kenya, access to financial services and products has

increased by around 56% between 2006-2019 driven by the availability of mobile money (Central Bank of Kenya, 2019). M-Pesa has also been credited with lifting roughly 2% of Kenyan households out of extreme poverty (Suri & Jack, 2016).

Image source: "M-PESA agent in Kibera, Nairobi" by Fiona Graham / WorldRemit is licensed under CC BY-SA 2.0

Clausewitz's Wallet

From the ashes of World War II, the U.S. dollar emerged as the dominant economic force. As the largest economy and the leader of the Free World, the U.S. was able to construct the dollar-based economic systems that route the world's transactions especially in the post–Bretton Woods world economy. Today, the U.S. is seeing its position erode having now dropped down to the world's second-largest trading partner. The U.S. has been militarily unchallenged since the demise of the Soviet Union and has used its position as a global economic as well as military superpower, using the dollar as a soft power Clausewitzian geo-political weapon. Clausewitz would clearly include in his "sum of the tools of statecraft," attaining financial dominance over an enemy (Miyata, 2021). Dominance in today's global financial system is enjoyed by the U.S. as the world's reserve currency, enabling leveraging the "payment rails" which facilitate cross-border financial transfers. The U.S.' influence on the SWIFT

network allows it to monitor global financial transactions and to wield the cudgel of economic sanctions, perhaps too frequently, to deter any challenges that may harm its national interests.

These sanctions can have serious impacts on the economies of countries affected by them. Once cut off from SWIFT's network, it becomes extremely difficult for a country to trade with the rest of the world. One recent example is Iran, which lost US$150 billion worth of revenue as a result of U.S. sanctions. Cross-border transactions made over payment rails like SWIFT are nearly always settled in dollars or involve a U.S. financial institution at some point. This payment rail dominance, combined with other dollar-based advantages, gives the U.S. a significant advantage over China, now the world's leading trading partner, as a tool for sanctions on Chinese companies, blocking transaction settlements through SWIFT (Reuters, 2020).

As of December 2021, countries sanctioned by the U.S. include Afghanistan, the Balkans, Belarus, Burma, Central African Republic, China, Cuba, Democratic Republic of Congo, Ethiopia, Hong Kong, Iran, Iraq, Lebanon, Libya, Mali, Nicaragua, North Korea, Russia, Somalia, Sudan and Darfur, South Sudan, Syria, Venezuela, Yemen, and Zimbabwe (OFAC, 2022). It is also noteworthy that many of the U.S. sanctions are unilateral rather than multilateral, enforcing crippling sanctions on countries without significant multilateral support. This cross-border financial foundation may not be as stable as the U.S. believe, and many countries harbor desires for alternatives.

With billions of people around the world already embracing new payment systems, or ready to move to non-Western dominated systems, dramatic change is possible, perhaps likely. The internet age has provided the evidence and the vehicle for financial system disruption, disintermediation, and a reshuffling of traditional relationships.

The Black Swan...or is it a Gray Rhino?

A "gray rhino" is a highly probable, high-impact yet neglected threat: kin to both the elephant in the room and the improbable and unforeseeable black swan. Gray rhinos are not random surprises but occur after a series of warnings and visible evidence. The fall of the Soviet Union, Climate Change, the 1928 and 2008 economic crashes, and even the advent of the internet age all exhibited signals well in advance heralding those events. We are now seeing a global financial great rhino in large part as a response to the U.S. government's threats to disconnect Russia from the SWIFT system. Russia has developed its own financial messaging system, called the System for Transfer of Financial Messages (SPFS) and banking card system (MIR). Russia's Deputy Foreign Minister, Alexander Pankin, stated that Russia echoes China's concerns around SWIFT being used as a geopolitical weapon by the West and that there is a need to modernize their payment methods (Bansal & Singh, 2021). Recently, Russia has also launched efforts to integrate SPFS and MIR with China's CIPS and UnionPay counterparts, as well as integrating SPFS across the Eurasian Economic Zone. China has built CIPS in twenty-five major countries, including the U.S., Singapore, Britain, France, Germany, South Korea, Russia, and Japan (Bansal & Singh, 2021). Yet risks to the financial system cut both ways, the German daily Die Welt wrote on February 27, 2022. "CIPS already handles US$50 billion of daily transactions. That is considerably less than the US$400 billion of transactions that pass every day through SWIFT, but CIPS volume has increased rapidly," the German

Image source: Stock Vector ID: 1888047045 by Maxim Gaigul (n.d.). Retrieved from: https://www.shutterstock.com/image-vector/rhino-hologram-rhinoceros-made-polygons-triangles-1888047045

newspaper reported. However, Die Welt concluded, "If Russia and China linked their systems and offered an alternative to other authoritarian states, this could threaten American domination of financial markets" (Reuters, 2022a).

Many members of the Chinese elite—even longtime advocates of market reform and economic opening—see a dark future for U.S.-China relations—and are increasingly focused on America's global financial hegemony as a long-term risk for their country. With China's growing wealth and prominence, they see the global economy as a legitimate area for defending their sovereignty and even as a way to retaliate (Gewirtz, 2019). The reality of financial war has been thrust upon the West in 2022 by Russia's return to war as a political tool resulting in the declaration, explicit or not, of near total economic war by the West. Notably absent from this economic coalition has been China, Brazil, India, and South Africa (the BRIC bloc) along with other countries unwilling to criticize their current or past patron. Will this be the catalyst to drive their adoption of an alternative to SWIFT and other Western-dominated financial networks?

On April 9th, 2022, Russia's Finance Minister, Anton Siluanov, told a ministerial meeting with BRICS, that they should integrate their payment systems. Sanctions have exacted a heavy toll on Russia's economy, losing access to more than US$600 billion of its gold and foreign exchange reserves (Reuters, 2022a). In 2017, Russia approved a cryptocurrency regulation framework, which would allow the government to "levy a 13% tax on individuals and organizations who attempt to trade their 'cryptorubles' for a flat currency but cannot demonstrate that the coins were obtained legally" (Kellerman, 2017). This policy reflects the Russian government's de-facto policy to profit from money laundering and other financial crimes as long as the victims are not Russian speakers.

Russia's political ruling class is indivisible from the oligarchs who have profited under Putin's rule. As much of the world has turned against Russia and imposed sanctions, increasing attention has been paid to the capital flight as they attempt to leak their funds out of the country. Without access to SWIFT and other sanctioned financial channels, these fund have sought out the weak spot in the global financial monitoring systems: decentralized

exchanges and the purchase of Non-Fungible Tokens or privacy coins (Gromek, 2022). Those are not their only options though: WebMoney, Yandex Money and Perfect Money are three of the larger Russian CVCs which enable money transfers around the world. In 2019, Sberbank said that WebMoney had joined its instant transfer ecosystem, allowing clients to connect their Sberbank accounts showing the degree of integration into the Russian banking system (Finextra, 2019). That integration was strangely interrupted on February 11th, 2022, when Russian authorities halted the ability to trade in rubles by revoking the license of their settling bank (Tass, 2022).

As of March 2022, Russia is actively trying to bypass SWIFT with its System for Transfer of Financial Messages (SPFS) developed by the Central Bank of Russia. SPFS has over 399 users, including more than 20 Belarusian banks, the Armenian Arshidbank, and the Kyrgyz Bank of Asia. Subsidiaries of large Russian banks in Germany and Switzerland have access to SPFS although this may change due to sanctions. Russia's central bank will stop disclosing the names of those participating in its alternative to the SWIFT payment system. Some Russian banks have been banned from the SWIFT banking system as part of the sweeping sanctions against the country over the Ukraine war. The ban has hampered cross-border transactions for Russia's trade and financial systems, isolating the country economically. The SPFS network extends beyond most Russian banks and now includes more than 50 foreign organizations (Reuters, 2022b).

Banks from Germany, Switzerland, France, Japan, Sweden, Turkey, and Cuba were among those connected to SPFS, according to a March 2022 report from Coface, a French credit insurer (Coface Economic, 2022). Until there was such a threat of being cut off from SWIFT, foreign partners were not in much of a rush to join, but now we expect their readiness to be greater," Nabiullina said of SPFS. An example is the Indian government's consideration of a Russian proposal to use the SPFS for payments in rubles, Bloomberg reported in March. India has been buying cargoes of cheap Russian oil amid international sanctions and boycotts of products from the energy powerhouse. Russian oil accounted for just 2% of India's total imports in 2021(Bloomberg News, 2022). Russia is currently negotiating with China to join the system. This alternative financial infrastructure enables Russian corporations and individuals to retain some access, albeit limited, to global markets despite sanctions (Liu & Papa, 2022). Should the other BRICS join SPFS and MIR, a viable, but limited alternative would exist with access to more than 3.23 billion people, which is over 40 percent of the world population.

This gray rhino may have a gray dragon close behind. As of end January 2022, there were 1,280 participants in China's Cross-border Interbank Payment Systems (CIPS), representing 103 countries and regions around the world.

However, this gray rhino may have a gray dragon close behind. As of end January 2022, there were 1,280 participants in China's Cross-border Interbank Payment Systems (CIPS), representing 103 countries and regions around the world. Participants include 11 foreign banks including some of the World's largest (DBS, Citibank, JPMorgan, Standard Chartered, HSBC, Deutsche, BNP Paribas, ANZ, MUFJ, Mizuho, and SMBC), 934 companies in Asia (541 companies in China), 159 companies in Europe, 43 companies in Africa, 29 companies in North America, 23 companies in Oceania, and 17 companies in South America. At least 23 Russian banks are connected to CIPS (as indirect participants), and Russia will have no trouble doing business in yuan through CIPS. Moreover, major

Russian private and state-owned institutions have only been accepting yuan payments in recent years. For instance, in September 2021, Gazprom switched from accepting U.S. dollar payments to yuan payments for aviation fuel. Although it has more participants than SPFS, its ubiquity is also not comparable to SWIFT (Coface Economic, 2022).

China has been working on an alternative to traditional "payment rails" as well. They have been working on their own digital currency since 2014, leading the world in efforts to field a large-scale Central Bank Digital Currency (CBDC). In 2016, the People's Bank of China (PBoC) successfully built the digital yuan prototype (e-CNY). At the end of 2017, the PBoC started the digital yuan research and development project, which saw participation from large commercial banks, internet companies, and telecommunications players. May of 2019 witnessed the launch of a large-scale pilot spanning four major cities in China. This was the first scale CBDC pilot in the world (Bansal & Singh, 2021).

In January 2022, the PBOC launched an app to allow users in 10 areas, including the major cities of Shanghai and Beijing, to sign up and use the e-CNY. The two dominant payment systems in China are Tencent's WeChat Pay and Alipay, which is run by Alibaba affiliate, Ant Group. Tencent announced that it would support the e-CNY in its WeChat Pay and Alipay which have over 1 billion users (Kharpal, 2022). The potential convenience of the e-CNY could extend WeChat Pay and Alipay's reach as the digital yuan can be used to make transactions without an internet connection, through proximity reading only. This could prove to be the digital yuan's most attractive feature, as it gives it helps digital payments act more like cash. As part of the e-CNY in Beijing, ATMs have been added to the city that convert the digital yuan to cash and vice versa (Zhao, 2021).

Many Other Central Banks are on the Move Too

Nine countries have launched CBDCs, another fifteen are in pilot stages, and sixteen are in development; the U.S. is NOT one of them. The Bahamas (their CBDC is named "Sand Dollar") along with the eight countries of the Eastern Caribbean Central Bank (ECCB) are among the first rolling out their CBDCs. The latter's pilot involves a securely minted and issued digital version of the Eastern Caribbean (EC) dollar, called DCash. Through this pilot the ECCU hopes to build resiliency from climate and political adversities, and create a more competitive economic system as well as broadening financial inclusion (ECCB, n.d.). This is, in part, to come up with alternatives to the correspondent banking which has been drying up in the region for over a decade due to a few Anti Money Laundering (AML) issues, and lingering perception issues, but mostly volume-to-profit problems that make the big banks not want to bother. This could be considered a response to the general de-risking trend from commercial banks.

Currently, the U.S. can monitor and regulate most global digital payment flows of dollars, but new payment systems could limit the ability of policymakers to track cross-border money flows. In the long term, the absence of U.S. leadership and standards-setting will have geopolitical consequences, especially if China maintains its first-mover advantage in the development of CBDCs. Considering the growing alternative payments ecosystem leadership shown by China (remember the US$60 trillion+ transaction value of Alipay and WePay), if combined

with their development of a viable CBDC, eventually a real financial (and law enforcement) nightmare could confront the West.

This battle is nowhere near lost, and indeed is just beginning. In a talk given to the Bank of England conference on "Central Banking and Fintech" in 2017, then head of the IMF Christine Lagarde (now the President of the European Central Bank) said that virtual currencies could actually become more stable than fiat currencies. She says, "for instance, they could be issued one-for-one for dollars, or a stable basket of currencies" while also leveraging the benefits of securely managed digital identities(Lagarde, 2017). However, in 2022, the current IMF Managing Director Kristalina Georgieva, has a less rosy vision, fraught with concern for "a world that could fragment into 'economic blocs', creating obstacles to the cross-border flow of capital, goods, services, ideas, and technologies" (Georgieva, 2022).

The respected payment guru David Birch shared his perspective that technology will be the key to providing secure transactions privately. Blockchain-based systems, "in particular, privacy-enhancing technology gives us the apparently paradoxical ability to keep private data on a shared or public ledger, which I think will form the basis of new financial institutions" (Birch, 2017).

Managing the Threat while Nurturing the Opportunity

"Our regulatory frameworks should be designed to support responsible innovation while managing risks—especially those that could disrupt the financial system and economy," U.S. Treasury Secretary Janet Yellen said recently in a speech on digital asset policy delivered at American University, arguing that new regulatory frameworks will be needed to manage those risks (Lawder, 2022).

U.S. President Biden's recent Executive Order requires the U.S. Department of the Treasury and U.S. Department of Commerce and other agencies to prepare reports on "the future of money" and the role cryptocurrencies will play (The White House, 2022). The internet, however, is not SWIFT. Regulation of the massive APE is not going to be as effective globally as regulators hope. With events in Ukraine driving a wedge into familiar Cold War fault lines, a schism is growing between familiar payment systems and new ones specifically created as an alternative to avoid regulation and oversight by the West.

The internet, however, is not SWIFT. Regulation of the massive APE is not going to be as effective globally as regulators hope.

Current financial intelligence systems rely upon signals being generated and detected through the network of financial institutions, including MSBs, submitted in the form of Suspicious Activity Reports (SARs). The efficacy of the SAR reporting system, and the ability of institutions like the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) to manage the flood of SARs (more than 2 million per year) limits the system's effectiveness, especially to detect new or unusual signals (Weiner Brodsky Kider PC, 2020). The SARs system also does not actively encourage the investigation

of secondary or tertiary connections that may be criminal usage indicators – especially in virtual currency use. While public blockchain intelligence systems like Chainalysis and CipherTrace are beginning to do "peel-chain" analysis where cryptocurrencies are exchanged for others to obfuscate their origins or usage, they do poorly when assessing where the money goes after conversion into a privacy coin, CVC, or other APS.

To understand where the money flows, as it moves through, into and out of the Alternative Payments Ecosystem (APE), a new Financial Open Source Intelligence (FOSINT) approach is required. Traditional follow-the-money approaches often miss the role played by the APE, especially when executed without a generalized understanding of this varied and constantly morphing set of companies and services.

Taming the APE: A Call to Action

As the use of the Alternative Payments Ecosystem (APE) continues to increase and diversify, so does the need to both encourage its development while enhancing systemic transparency. Our institutional abilities to expose adversarial and criminal applications require innovation. This includes not only the tech and financial industries, but policymakers and regulators alike. Incentives must be created for fintech firms to limit their 'operational risks' through the implementation of KYC/AML protocols. Incentives, or conversely disincentives, should also be created to limit the de-risking of APS such as remitters, as these systems provide vital lifelines to beleaguered and impoverished populations from Somalia to Ukraine to Guatemala.

The U.S. needs to follow our private sector's global technology leadership by setting the standards for the APE in the international arena. Regardless of whichever direction the U.S. government takes the digital dollar, CBDCs, stablecoins, eCash, or other new payment technologies, it cannot wait to engage the world through international organizations. To wait for a domestic decision may mean ceding leadership of FATF, waiting for the BRICs to create a viable alternative to SWIFT, or ignoring arenas where China and others are dominating (such as mobile or CVCs) and thus setting the standards that might be used for law, regulation, interoperability, digital illiberalism, and integrated digital payment systems. Instead, this leadership should extend beyond regulations, law enforcement, and Counter Threat Finance (CTF) to using the APE to enable financial inclusion. Offering greater support to the World Bank's Financial Inclusion Global Initiative (World Bank Group, 2021) through the U.S. Agency for International Development (USAID) would be a good place to start.

When we do need to create laws and regulations to manage the illicit use of the APE, it is critical that legislators be better educated and have permanent committee staff who are expert on these topics. With bad actors and adversaries gaining leverage quickly, Congress must be serious about the risks and opportunities of the APE, in part by committing to understanding the terms and embracing realistic solutions to the risks of this evolving financial system. These include weaknesses with investor and consumer protection and the ongoing or potential abuse of the APE by our adversaries, including criminals and nation-states. Differences between political parties and jurisdictional debates (e.g., whether a cryptocurrency is a security, a deposit, or a commodity) have resulted in a constant, but unproductive, legislative churn.

Authorities for regulatory agencies need to be modernized to enforce the existing laws, as well as prepare for new ones that need to be written. Many current laws and regulations were written for traditional banking systems (SWIFT and ACH) and are ill-suited for managing the APE. Blocking actions by FinCEN, for example, can only be applied to "correspondent banking or payable-through accounts." Technically, as it currently stands, its outdated special measures authorities cannot be applied to a VCE, remittance system, any kind of MSB, or other cross-border transfer system if and when FinCEN and partner agencies find an entity to be a "Primary Money Laundering Concern." Modernized authorities like this are critical if our regulators are to be effective in oversight and engagement of the APE.

The following are possible ways to enable the U.S. to better cope with the threat and opportunity provided by the APE:

- Education of law enforcement investigators and intelligence analysts in APE and how it integrates with criminal and adversary systems. Regulators including the Security and Exchange Commission (SEC), the Financial Crimes Enforcement Network (FinCEN), as well as policy makers in various Executive Agencies, and the US Congress must understand these issues better as well. This should also include creating a common APE lexicon across agencies, law, and regulation.
- Financial Open Source Intelligence (FOSINT) platforms must be created and synthesized with existing OSINT tools. These platforms must look beyond blockchain analysis systems for cryptocurrencies and integrate with all available data on non-public blockchain-based VCs, including CVCs, MPSs, and Remitters. This would include creating new Internet collection and analysis tools and combine with other data (e.g., law enforcement data, SARs, or proprietary financial institution data).
- Regulations should be modernized to support the Financial Action Task Force (FATF) prioritization of including VCEs in Country Scorecards. These regulations should also encourage policy and incentives for banks to end de-risking practices which hurt the poor and drive illicit payments further underground.
- Government FININT coordination through the creation of a "National Counter Threat" capability through the Office of the Director of National Intelligence (ODNI). By providing a central point for collaboration and data sharing this capability would include all aspects of national intelligence and law enforcement. This new function could be part of a modified National Counter Terrorism Center (NCTC) with a mission to examine the intersection of crime, terrorism, and nation state threats across all the ODNI Centers (NCTC, CTIIC, NCPC, NCSC).

Without an integrated and comprehensive approach, the APE will continue to grow and strengthen. If that day comes—and it could arrive sooner than most think—the West's ability to dominate the world's financial sphere of soft power will lessen. Without action, our ability to live in a rules-based financial system will fade with it.

About the Author

The opinions expressed here are those of the author and do not represent the Wilson Center.

Scott Dueweke, Global Fellow, The Wilson Center's Science and Technology Innovation Program

Scott Dueweke is an expert on *identity*, the *blockchain*, the *dark web* and *alternative payment systems* at Leidos and in 2021 was appointed as a Global Fellow at the Wilson Center. He has advised senior leadership within financial institutions, the U.S. government, as well as international law enforcement. In 2012 he sparked the Silk Road dark market investigation by the US Secret Service while presenting at a EUROPOL money laundering conference. Mr. Dueweke has provided training on digital identity, the blockchain and other digital value systems to non-profits, corporations and governments, including Citigroup, the National Health Care Innovation Summit, the US Intelligence Community, FBI, Department of State, USAID, INTERPOL, EUROPOL, and the UNODC to name a few. Through his knowledge of the Dark Web and anonymous payments he supported Operation Underground Railroad in their efforts to stop global child sex slavery rings. In June 2018 Mr. Dueweke testified on the role of anonymous payment systems in allowing foreign influence on US elections, and in 2017 on cybercrime before the House Banking Committee.

Mr. Dueweke has provided public and private sector clients an understanding of identities and alternative payment systems, both risks and rewards. In 2015 he provided *Anti-Money Laundering (AML)* and *Counter Terrorism Funding (CTF)* training for more than 40 countries' Financial Intelligence Units (FIU) including sessions in the Philippines, Turkmenistan, Kazakhstan and Turkey. He helped lead, along with the US Department of State's Counter-Terrorism Bureau and USAID, the New Payment Systems Workshop at the Asia Pacific Economic Cooperation (APEC) Senior Leaders Working Group at Subic Bay, Philippines.

He began his career with the U.S. Agency for International Development, where Mr. Dueweke contributing to the Armenian earthquake and Hurricane Gilbert responses. He also co-founded Freedom Flight International in the mid-1990s where, working with the U.S. Coast Guard, his organization flew private aircraft over the Florida Straits to assist the rescue of Cuban rafters as profiled in the book, "Dying to Get Here: A Story of Coming to America".

References

Bansal, R & Singh, S. (2021, August 31). China's Digital Yuan: An Alternative to the Dollar-Dominated Financial System. Carnegie India. Retrieved May 22, 2022, from https://carnegieendowment.org/files/202108-Bansal_Singh_-_Chinas_Digital_Yuan.pdf

Birch, D. G. W. (2017, October 3). Don't listen to me, listen to Christine Lagarde. 15Mb. Retrieved May 22, 2022, from https://blog.dgwbirch.com/?p=211

Bloomberg News. (2022, April 19). Russia Touts SWIFT Alternative, But Will Keep Its Members Secret. Bloomberg News. Retrieved May 22, 2022, from https://www.bloomberg.com/news/articles/2022-04-19/russia-touts-swift-alternative-but-will-keep-its-members-secret

Coface Economic (2022, March). Economic Consequences of the Russian-Ukraine conflict: Stagflation ahead. Coface Economic. Retrieved May 22, 2022, from https://www.cofacegk.no/ResourceServlet/i70c5f1f-7a4c41ce927243eff6e2222c

Central Bank of Kenya. (2019, April 14). 2019 FinAccess Household Survey. Central Bank of Kenya. Retrieved May 22, 2022, from https://www.centralbank.go.ke/uploads/financial_inclusion/1035460079_2019%20FinAcces%20Report%20(web).pdf

ECCB. (n.d.). About the Project. Eastern Caribbean Central Bank. Retrieved May 22, 2022, from https://www.eccb-centralbank.org/p/about-the-project

FATF. (2021, June 25). Outcomes FATF plenary, 20-25 June 2021. Financial Action Task Force (FATF). Retrieved May 22, 2022, from https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2021.html

Finextra. (2019, February 22). Sberbank customers can now transfer money from their cards using recipient phone number. Finextra Research. Retrieved May 22, 2022, from https://www.finextra.com/pressarticle/77372/sberbank-customers-can-now-transfer-money-from-their-cards-using-recipient-phone-number

Georgieva, K. (2022, May 10). Confronting fragmentation: How to modernize the international payment system – Speech. Eurasia Review. Retrieved May 22, 2022, from https://www.eurasiareview.com/10052022-confronting-fragmentation-how-to-modernize-the-international-payment-system-speech/

Gewirtz, J. (2019, December 17). Look out: Some Chinese thinkers are girding for a "Financial War". POLITICO. Retrieved May 22, 2022, from https://www.politico.com/news/magazine/2019/12/17/look-out-some-chinese-thinkers-are-girding-for-a-financial-war-086610

Gromek, M. (2022, April 27). Wrestling russia on the blockchain - six most likely sanctions to be imposed. Forbes. Retrieved May 22, 2022, from https://www.forbes.com/sites/michalgromek/2022/04/27/wrestling-russia-on-the-blockchainsix-most-likely-sanctions-to-be-imposed/?sh=a176803e1885

Hern, A. (2020, November 4). Silk road bitcoins worth $1bn change hands after seven years. The Guardian. Retrieved May 22, 2022, from https://www.theguardian.com/technology/2020/nov/04/silk-road-bitcoins-worth-1bn-change-hands-after-seven-years

IFAD. (2015, September). The use of remittances and financial n=inclusion. International Fund for Agriculture Development (IFAD). Retrieved May 22, 2022, from https://www.ifad.org/documents/38714170/40187309/gpfi.pdf/58ce7a06-7ec0-42e8-82dc-c069227edb79

Kellerman, T. (2017, November). Follow the Money: Civilizing the Darkweb Economy. Wilson Center. Retrieved May 22, 2022, from https://www.wilsoncenter.org/sites/default/files/media/documents/publication/dfp_follow_money_kellermann.pdf

Kellerman, T. & McElroy, R. (2021). Modern Bank Heists 4.0. VMware. Retrieved May 22, 2022, from https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-modern-bank-heists-2021.pdf

Kharpal, A. (2022, January 11). China is pushing for broader use of its digital currency. CNBC. Retrieved May 22, 2022, from https://www.cnbc.com/2022/01/11/china-digital-yuan-pboc-to-expand-e-cny-use-but-challenges-remain.html

Lagarde, C. (2017, September 29). Central Banking and Fintech-A Brave New World? IMF. Retrieved May 22, 2022, from https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world

Lawder, D. (2022, April 7). Yellen says U.S. crypto rules should support innovation, manage risks. Reuters. Retrieved May 22, 2022, from https://www.reuters.com/business/finance/yellen-says-us-crypto-rules-should-support-innovation-manage-risks-2022-04-07/

Liu, Z. Z., & Papa, M. (2022, May 18). The Anti-Dollar Axis. Foreign Affairs. Retrieved May 22, 2022, from https://www.foreignaffairs.com/articles/russian-federation/2022-03-07/anti-dollar-axis

Miyata, F. (2021, March 26). The grand strategy of Carl von Clausewitz. War Room - U.S. Army War College. Retrieved May 22, 2022, from https://warroom.armywarcollege.edu/articles/grand-strategy-clausewitz/

Notabene. (2022). The "Sunrise Issue" of the Crypto Travel Rule. Notabene. Retrieved May 22, 2022, from https://notabene.id/sunrise-issue#:~:text=The%20FATF%20recognizes%20the%20compliance,at%20which%20their%20counterparties%20operate.

OFAC. (2022). Sanctions Programs and Country Information. U.S. Department of the Treasury. Retrieved May 22, 2022, from https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

O'Gardy, V. (2021, September 7). M-Pesa hits the 50 million mark. Developing Telecoms. Retrieved May 22, 2022, from https://developingtelecoms.com/telecom-technology/financial-services/11851-m-pesa-hits-the-50-million-mark.html

O'Neill, A. (2021, November 26). Total population of the BRICS countries 2026. Statista. Retrieved May 22, 2022, from https://www.statista.com/statistics/254205/total-population-of-the-bric-countries/#:~:text=In%202021%2C%20it%20is%20estimated,percent%20of%20the%20world%20population.

PYMNTS. (2021, September 24). China Widens Mobile Payments antitrust probe. PYMNTS.com. Retrieved May 22, 2022, from https://www.pymnts.com/antitrust/2021/china-widens-mobile-payments-antitrust-probe/

Rappeport, A. (2021, April 13). Tax cheats cost the U.S. $1 trillion per year, I.R.S. chief says. The New York Times. Retrieved May 22, 2022, from https://www.nytimes.com/2021/04/13/business/irs-tax-gap.html

Redman, J. (2022, April 4). Bitcoin cold case: The tale of the dormant wallet with close to 80,000 BTC from Mt Gox. Bitcoin News. Retrieved May 22, 2022, from https://news.bitcoin.com/bitcoin-cold-case-the-tale-of-the-dormant-wallet-with-close-to-80000-btc-from-mt-gox/

Reuters. (2020, July 29). Chinese banks urged to switch away from Swift as U.S. sanctions loom. Reuters. Retrieved May 22, 2022, from https://www.reuters.com/article/us-china-banks-usa-sanctions/chinese-banks-urged-to-switch-away-from-swift-as-u-s-sanctions-loom-idUSKCN24U0SN

Reuters. (2022a, April 9). Russia calls for integrating BRICS payment systems. Reuters. Retrieved May 22, 2022, from https://www.reuters.com/business/finance/russia-calls-integrating-brics-payment-systems-2022-04-09/

Reuters. (2022b, April 19). Russia Central Bank will not name banks linked to swift alternative. Reuters. Retrieved

May 22, 2022, from https://www.reuters.com/world/europe/russia-central-bank-will-not-name-banks-linked-swift-alternative-2022-04-19/

Roberts, J. J., & Rapp, N. (2017, November 25). Exclusive: Nearly 4 million bitcoins lost forever, new study says. Fortune. Retrieved May 22, 2022, from https://fortune.com/2017/11/25/lost-Bitcoins/

Sharma, R. (2022, April 16). North Korean attackers snipes Axie Infinity Gamers in $620 million burgle: FBI. The Coin Republic. Retrieved May 22, 2022, from https://www.thecoinrepublic.com/2022/04/16/north-korean-attackers-snipes-axie-infinity-gamers-in-620-million-burgle-fbi/

Suri, T., & Jack, W. (2016, December 9). The long-run poverty and gender impacts of Mobile Money. Science, 354(6317), 1288–1292. https://doi.org/10.1126/science.aah5309

Tass. (2022, February 11). WebMoney halts operations with Russian wallets from February 11th. Tass. Retrieved May 22, 2022, from https://tass.com/economy/1401755?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

The White House. (2022, March 9). Executive order on ensuring responsible development of Digital assets. The White House. Retrieved May 22, 2022, from https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

U.S. Department of Justice. (2016, August 10). Liberty Reserve founder sentenced to 20 years for laundering hundreds of millions of dollars. The United States Department of Justice. Retrieved May 22, 2022, from https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars

U.S. Department of Justice. (2022, February 8). Two arrested for alleged conspiracy to launder $4.5 billion in stolen cryptocurrency. The United States Department of Justice. Retrieved May 22, 2022, from https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

Ventura, L. (2021, February 17). World's most unbanked countries 2021. Global Finance Magazine. Retrieved May 22, 2022, from https://www.gfmag.com/global-data/economic-data/worlds-most-unbanked-countries

Weiner Brodsky Kider PC. (2020, October 13). FinCEN's data shows continued increase in SAR filings. JD Supra. Retrieved May 22, 2022, from https://www.jdsupra.com/legalnews/fincen-s-data-shows-continued-increase-58306/

World Bank Group. (2021, March 10). Financial Inclusion Global Initiative (FIGI). World Bank. Retrieved May 22, 2022, from https://www.worldbank.org/en/topic/financialinclusion/brief/figi

Zhao, W. (2021, February 18). Beijing's new digital yuan test features ATMs that convert digital currency to cash. The Block. Retrieved May 22, 2022, from https://www.theblockcrypto.com/post/95266/beijing-digital-yuan-cash-

WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

The Wilson Center, chartered by Congress in 1968 as the official memorial to President Woodrow Wilson, is the nation's key non-partisan policy forum for tackling global issues through independent research and open dialogue to inform actionable ideas for the policy community.

THE SCIENCE AND TECHNOLOGY INNOVATION PROGRAM (STIP)

The Science and Technology Innovation Program (STIP) brings foresight to the frontier. Our experts explore emerging technologies through vital conversations, making science policy accessible to everyone.

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

The Wilson Center

www.wilsoncenter.org
wwics@wilsoncenter.org
facebook.com/woodrowwilsoncenter
@thewilsoncenter
202.691.4000

STIP

www.wilsoncenter.org/program/science-and-technology-innovation-program
stip@wilsoncenter.org
@WilsonSTIP
202.691.4321

Wilson Center

Science and Technology Innovation Program

Responses to Questions for the Record Submitted to
Subcommittee on National Security, International Development, and Monetary Policy

Hearing entitled, "Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth"

Tuesday, September 20, 2022, at 10:00 a.m.

Emily Jin
Research Assistant
Energy, Economics, and Security Program
Center for a New American Security

1. Increased interoperability of alternative cross border payment systems could trigger a scenario where regional economies operate cross-border systems and settle transactions in currencies other than U.S. dollars, euros, or sterling. IMF Managing Director Kristalina Georgieva argues that this could create, "obstacles to the cross-border flow of capital, goods, services, ideas, and technologies."

    a. In your opinion, how could non-dollar denominated, regionalized payment systems affect U.S. regulators' ability to monitor cross-border flows?

    Because non-dollar denominated and regionalized payment systems operate under authorities outside of the United States, they are harder to monitor on default. Moreover, they may not be transparent with disclosing institutions using their services and transaction flows. In China's case, CIPS at least still publishes monthly volume data on their home page and include participating institutions' names on the site. In Russia's case, the Russian central bank recently announced in April 2022 it will cease disclosing names of organizations that use its System for Transfer of Financial Messages (SPFS). As of June 2022, the Russian central bank announced that 70 organizations from 12 countries have joined its payment system, but stopped short of disclosing names out of concern about secondary sanctions. It is not a far stretch to assume more organizations might join SPFS in the future, though they would likely be concerned about being perceived as helping Russia evade sanctions.

    b. Could a system or series of systems like this help authoritarian regimes finance their efforts and evade traditional economic sanctions imposed by the U.S. and our allies?

    Yes, a series of systems could help authoritarian regimes finance their efforts and partially evade traditional economic sanctions imposed by the United States and its allies. Though, it would require meaningful coordination and high interoperability between the systems. Even with high levels of coordination and interoperability, it would be more apt to describe the the extent of sanction evasion in the short-term as pressure "release valves" for bad actors, as opposed to full mitigation of the sanctions. As of now, there may be efforts to coordinate. However, it remains unclear whether these payment systems are interoperable with one another.

2. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) network is the most widely used messaging system for cross-border payments between financial institutions. Following Russia's illegal invasion of Ukraine in February 2022, the European Unions, the United Kingdom, Canada, and the U.S. agreed to remove seven Russian banks from the SWIFT network.

    a. What other cross-border payment mechanisms has Russia sought to replace the utility of the SWIFT network?

    In the last few years, Russia has been developing payment processing capabilities to reduce reliance on dollar-centered payments infrastructure. The Mir payment system and cards were created to respond to U.S.-led global payment processing ecosystem denying services to Russian banks under U.S. sanctions after Russia's first invasion of Ukraine in 2014. After Visa, Mastercard, and China's UnionPay backed out of Russia in May 2022, Mir cards increased their adoption among both domestic and international audiences, though the international user base is limited to a couple of countries and territories within the Russian sphere of influence and control.

    The System for Transfer of Financial Messages (SPFS) was created also to address U.S. threat of removing key Russian banks from the SWIFT network. The Russian government has explored connecting its payment system to other countries' counterparts, such as the Turkish and Iranian payment systems. Moreover, Russian authorities are pushing for select countries to accept Mir card payments. Interestingly, though some Turkish banks adopted Russia's Mir payments system in August 2022, all Turkish state-owned banks suspended their use of Russian mir payment system in September 2022. This demonstrates that the use of Mir and SFPS is generally constrained to domestic Russian audiences and sometimes in countries that are under Russia's geopolitical influence. Though, these countries may be concerned about the costs of connection.

    b. Have other countries looked to join alternatives to SWIFT in the wake of the sanctions imposed on Russia?

    While there are purportedly institutions that joined SPFS after the waves of sanctions, the names of institutions are not disclosed (a practice the Russian authorities implemented since April of 2022). Some countries are contemplating joining China's CIPS. Belarus for example have announced it will join CIPS in the medium term, without specification on the exact year or date.

3. We have heard testimony today that widespread international adoption of these alternative payment systems is unlikely in the immediate future. The Russian ruble is volatile, and the Chinese government has imposed strict capital limitations on the RMB.

    a. Why is the alternative payments ecosystem a potential threat to the U.S. and our allies?

    There are two potential future scenarios, and both require attention of the U.S. and allies. First, if enough alternative financial rails coalesce into a critical mass that provides escape valves for sanctioned entities, these entities may be able to trade on alternative payment systems. The level of these transactions might not meaningfully help sanctioned entities evade the power of U.S. economic and financial sanctions, but this would warrant vigilance from the U.S. and our allies.

    Second, if the Chinese leadership makes painful political and economic reforms down the line and liberalizes its capital account, the RMB might just become a more appealing store of value. Over time, Chinese payment systems and financial rails could over time garner critical mass in adoption. This very low-likelihood event may not happen for many years, so once it takes place, China would have had years to fine-tune and perfect its payment systems and financial rails. Foreign financial institutions and firms may be compelled to adopt CIPS clearing and settlement, as they likely would not want to miss out on participating in China's market and alternative systems. CIPS and other Chinese financial mechanisms and digital innovations could put China in a stronger position to connect with other alternative financial rails and notes. This may ultimately empower China to challenge the United States' economic and financial leadership.

    b. Is it only a threat if Russia and China build more robust global economic ties and volume?

    No, it is also a U.S. national security threat given the possibility for a coordinated coalition of alternative payment systems down the line. In a world where blocs have formed along more distinct lines, authoritarian countries may become accustomed to working with one another to mitigate the political and economic penalties from international condemnation. In anticipation for that future, policymakers must closely monitor the patchwork of alternative payment rails and nodes. In the meantime, the United States and allies and partners must be in regular dialogues to facilitate information-sharing and develop the muscle for policy coordination.

4. In the past decade we have seen an increase in alternative payment systems. China introduced their Cross-Border Interbank Payment System and Russia developed their System for Transfer of Financial Messages (SPFS) and Mir to process payments.

    a. What are the economic benefits or costs of maintaining a robust alternative payment system?

    The economic benefits for users of robust payment systems include reduced friction and costs in international payments, which arise from currency conversions, varied tax regimes, and processing fees. It is unclear what economic benefits are afforded to the host country of this payment system, besides intangibles such as greater influence in global financial leadership. I have not conducted the requisite research for a comprehensive cost analysis of maintaining a robust alternative payment system. I endeavor to research that line of inquiry in the future.

    b. What is the relationship between a strengthening Chinese payment system and RMB internationalization?

    RMB internationalization can only happen if China makes structural changes to its political economic system (e.g. liberalizing its capital account, eliminating social repression, and becoming a more responsible international actor). The world would have to find the Chinese political economic model appealing and stable enough before entrusting to store their value in the RMB. Only in such a scenario, would the Chinese payment system be potentially adopted on a broader scale. To be clear, China is highly unlikely to change its political and economic model in the foreseeable future, as long as the leadership's calculus around social control and financial stability outweighs its ambition for a more internationalized RMB.

5. China introduced the Cross-Border Interbank Payment System in 2015 to more efficiently settle and clear RMB transactions. Today CIPS services 1,280 financial institutions across 103 countries.

    a. What are PRC's intentions in maintaining CIPS and other alternative financial plumbing, rails, and nodes?

    For CIPS, the PRC likely has intentions to normalize the use of RMB in cross-border clearing and settlement. The PRC likely has plans to enhance the functionality of CIPS so that it will eventually rely on SWIFT less. This would allow the PRC to diversify its financial rails or "attachments" to global financial plumbing.

    As for the eCNY, the PRC's intentions are more domestic in the near term. The PRC wants to digitize its economy to aid in its development goals, while also build an extensive infrastructure for improved social control. However, the potential cross-border applications are obvious. It would be naïve to think the PRC will stop at integrating eCNY just within its borders and have no ambition for international adoption. In the medium to long terms, the PRC likely will encourage usage of the eCNY in cross border transactions, which has serious implications for the economic competitiveness of U.S. companies that wish to operate inside the Chinese market.

    b. How should the United States respond to these developments in the PRC?

    In my testimony, I provide seven recommendations to the U.S. government. I will highlight just one recommendation in response to this question, though all are crucial. The United States must engage proactively in standard setting bodies for digital assets and financial rails. According to the recently released Comprehensive Framework for Responsible Development of Digital Assets, the United States government is considering policy objectives for a U.S. CBDC system. While it is unclear the United States would be pursuing a digital dollar, the government should be tracking and consistently assessing the impact of licit and illicit digital assets on the strength and integrity of the U.S. financial system. The United States needs to be not just participating but driving the standard-setting discussion around alternative financial plumbing, rails, and nodes. This means driving discussions at convenings hosted by the Bank for International Settlements (BIS), and other standard organizations such as the International Organization for Standards (ISO).

6. Mobile wallet applications have consistently made up more than 40% of global e-commerce value and are projected to account for more than half of all transactions by 2025.

    a. What is driving the growth of these alternative payment systems?

    Mobile wallet applications have grown amid globalization, with the mobile wallet market size expected to reach $30.2 billion by 2028 growing at rate of 27% CAGR from 2022. The growth of these alternative payment systems is driven by increased e-commerce activity, as well as rising use in smart phones around the globe. Government efforts in expand digital penetration (such as Digital India) have also contributed to the rising trend of mobile wallets.

    b. These systems can pose greater threats when they grow in size and volume, and when they might become interoperable. What are some of the issues that would require a U.S. and allied response?

    As always, technologies present positive and negatives for AML/CFT purposes. One positive is that these applications facilitate and deepen global flow of commerce. One clear negative is that there have been growing cases of cyber vulnerabilities across the world. If illicit financial activities are increasingly carried out via mobile wallet applications, the United States and allied governments must spring to action. The intergovernmental Financial Action Task Force (FATF) provides a good model for developing and coordinating policies. The United States and allied governments need to coordinate to refine and implement measures that would prevent and mitigate abuses of alternative payment systems by bad actors.

7. Non-U.S. mobile payment applications reportedly reach more than 1 billion consumers and process over $60 trillion worth of transactions worldwide. Continued advancement of these products into foreign markets can diminish U.S. competitiveness and yield opportunities for foreign governments to influence international payment principles.

    a. How can Congress help promote and encourage participation of U.S.-based payment companies in foreign markets?

    Congress should routinely meet with U.S.-based payment companies and with officials from the U.S. Trade Representative and other relevant government agencies and offices to understand industry trends and the extent of market access that the United States has secured in foreign markets. Using China as an example, even though China has agreed to opening up its markets for U.S.-based payment companies, it has not followed through on these commitments. The United States government as a whole needs to continue to secure market access for U.S. payment companies in foreign markets, though some may be much more difficult than others to negotiate.

    b. What regulatory standards should policymakers consider to ensure that U.S. companies remain competitive in the international payment sector?

    U.S. regulation in the payments space should mandate that private companies prioritize security and efficiency of their services. U.S. regulation should also encourage innovation, while also ensuring that technological advancements are properly aligned with national security objectives.

8. The growth and expansion of alternative cross-border payment systems could lead to a world less dependent on U.S. dollars, which would likely limit our traditional methods of economic sanctions.

    a. How should U.S. national security experts be preparing our sanctions toolkit to respond to this scenario?

    The Treasury Department should be in close coordination with financial institutions. Specifically, there should be information-sharing on the developments within the alternative payment ecosystem. Banks are on the front lines of sanctions enforcement, so timely information dissemination is crucial.

    In terms of the sanctions toolkit, the Treasury Department may need to consider levying secondary sanctions on entities that elect to connect directly to the CIPS network. This should only be levied in cases where there is reasonable doubt that sanctions evasions are afoot. Before levying such secondary sanctions, the department should conduct impact analysis and anticipate potential secondary effects from such sanctions.

    b. What are some examples of nonfinancial sanctions measures that could act as a deterrent in the same way that financial sanctions do today?

    Sectoral sanctions imposed on specified persons or entities could deter illicit activity. I have not conducted the requisite research to make judgement on the effectiveness of sectoral sanctions compared to financial sanctions.

9. Sanctions that are made possible because of the strength of the U.S. dollar could push countries to reduce their use of U.S. dollars and minimize the global economic power of the United States. Although the dollar will likely be the world's primary reserve currency for the foreseeable future, governments could experiment with other national currencies to proactively shield their economies from the U.S.

    a. How long could a government successfully sustain itself without using currencies like dollars, euros, or sterling?

    This would depend on the level of coordination between the United States, the European Union, the United Kingdom, and other major economies. If the targeted government is highly dependent on global trade, it likely would be using the dollar, euro, and/or sterling to underwrite most of its trade. If all these currencies become unavailable to the sanctioned government (or at least, much harder to transact with), the sanctioned government could certainly feel the pain quickly after sanctions. However, this would also depend on whether the sanctioned government has a current account surplus. If it does, it could potentially use that surplus to defend its economy and support its spending (fortress economics). There are a host of other variables at play, but my analysis would start at assessing the sanctioned government's dependence on global trade, then evaluate their current account surplus and investigate the extent to which the sanctioned government has developed a fortress economy.

    b. What inflection points would signal that major economies are attempting to de-dollarize? How should U.S. policymakers address that scenario?

    China and Russia are de-dollarizing. As discussed in detail in my testimony, China and Russia have been de-dollarizing on their own (China reducing its dollar holdings in its foreign exchange reserves from 79% in 1995 to 59 percent in 2016; Russia reducing its dollar holdings from 40% n 2017 to 16% in 2021), but also have collectively reduced their reliance on the U.S. dollar via bilateral trade currency settlements. Notwithstanding some progress in de-dollarizing separately and jointly, China and Russia are unlikely to meaningful build a global de-dollarized coalition that can challenge the mainstream financial system, as the U.S. dollar is still a center of gravity in the global financial system. Inflection points would be clear evidence that many foreign banks have started to transact using China's CIPS and/or Russia's SPFS, and that CIPS and SPFS start to integrate their systems. In those cases, U.S. policymakers may need to consider defensive policy options and impose restrictive measures on U.S. entities using alternative payment systems.

10. In April, the Russian Minister of Finance proposed that Brazil, Russia, India, China and South Africa integrate their payment systems to promote greater use of Mir and domestic currencies in cross-border financing.

    a. Do you believe this is likely to happen?

    BRICS countries have opened currency swap lines to settle trade with their own currencies, so that is already happening. However, it is unlikely that BRICS countries would have integrated payment systems, as doing would likely be too costly politically. I am also skeptical that there would be wide adoption of the Mir cards in BRICS, given again the alarming signals that would send to the U.S. and allies. However, I am not precluding this as a possibility in the medium to long terms.

    b. How would this mitigate the impact of Ukraine-related economic and trade sanctions?

    Mir cards are allegedly difficult to use and have limited international operationality. SPFS has minuscule volumes and lackluster functionality compared to SWIFT. The lacking functionality, use cases, and political costs make BRICS payment systems integration and broader Mir usage an uphill battle. Hence, the fundamental economic pressures facing Russia are not going away.

11. One of the benefits of the SWIFT network is that SWIFT messages are standardized, secure, and relatively inexpensive, helping connect 11,000 financial institutions across more than 200 countries. However, competing cross-border messaging and clearing systems may challenge SWIFT's leadership, complicate international finance, and make it difficult for U.S. regulators to track illicit flows.

    a. How complicated is it to create a network that is similar and comparable to SWIFT?

    I have not conducted enough analysis to provide a detailed list of requirements for creating a network comparable to SWIFT. One requirement would be for the alternative network to have a messaging system that is technically reliable to be used across financial institutions around the world. While I am unsure how complicated it is to create a financial messaging system, alternative payment systems may face headwinds in convincing financial institutions to use their messaging services, as most financial institutions use SWIFT's messaging.

    b. Should we anticipate that a major competitor to SWIFT could be developed in the near future, and if so, how should national security and financial intelligence professionals prepare for that shift?

    We should not anticipate that a major competitor to SWIFT could be developed in the near future, as the closest alternative payment system in terms of transaction volume (China's CIPS) is still magnitudes smaller than SWIFT. Moreover, China's CIPS is functionally different from SWIFT, as it clears and settles the RMB as opposed to serving as messaging system for global financial institutions. However, U.S. national security and financial intelligence professionals need to monitor developments in the alternative payment ecosystem and focus on innovating in the payments space so that the United States can maintain a prominent position in the payments industry.

12. In 2014, Russia began developing its own financial messaging and banking card systems after the U.S. imposed strict sanctions in response to Russia's illegal annexation of the Crimean Peninsula. These systems allow Russia to continue processing domestic payments, though cross-border options. They also allow access to currencies widely used in international transactions that are limited due to the sanctions imposed by the U.S. and allies after Russia's illegal invasion of Ukraine in February 2022.

    a. How have Russia's financial messaging and banking card systems helped insulate its economy from sanctions?

    The Russian government has explored connecting the SPFS to other countries' payment systems, such as Turkish and Iranian payment systems. Moreover, Russian authorities have pushed for select countries to accept Mir card payments. Despite these efforts, Russia's financial messaging and banking card systems are only providing minimal relief, mostly limited to the domestic audience.

    b. What is the likelihood that other countries may look to replicate Russia's payment system strategy to defend their economy from economic sanctions?

    Russia has employed a fortress economics strategy by generally maintaining a current account surplus so it can support its spending when sanctions bite. Its payment system strategy is a sub-category of its general fortress economics strategy. Policymakers (in China but also elsewhere) may take note of this strategy. China has been using a fortress economics strategy as well, as it wants to increase its exports and reduce reliance on imports. This is demonstrative in China's Dual Circulation Strategy, where it wants to continue to export its excess capacity, while developing indigenous capabilities so it can overtime reduce its reliance on imported critical technologies and inputs.

13. Many alternative payment systems are domiciled or operating in nations with anti-money laundering standards that are not as strict as those proposed by the Financial Action Task Force and U.S. law and regulations. This means that in many cases, transactions are processed without any attempt by the operator to know the customers on each end of the transactions. The result is that financial crime, including money laundering and sanctions evasion, can occur in plain sight.

    a. Are know your customer (KYC) checks effective for these alternative payment systems?

    At the present time, I have not conducted the necessary analysis to assess whether current KYC checks are effective at screening transactions via alternative payment systems. I echo the concern from the question that uneven anti-money laundering standards across different payment systems make detecting financial crime difficult. This is an important question that I endeavor to take on in future research.

    b. Do they need to be implemented in all systems, why or why not, and what are examples of where such standards could be useful to America's national security interests?

    I have not conducted the necessary analysis to make an extensive response to this question.

14. Some national security experts predict that authoritarian governments will leverage digital payment infrastructure and central bank digital currencies as a tool for economic coercion and global data surveillance.

    a. How do alternative payment rails play a role in countries' political and economic strategies?

    In acute geopolitical scenarios, alternative payment rails could provide countries economic relief valves when under sanctions pressure. In a long-term outlook, a critical mass of alternative payment rails could coalesce into a coalition of alternative financial rails and nodes, which could erode the power of U.S. and allied economic and financial sanctions.

    b. Can an efficient and inexpensive payment system be a soft power tool and further limit participation of U.S. payment companies?

    An efficient and inexpensive payment system can be a soft power tool, but this is predicated on the host country of the payment system having a political and economic system that is attractive to potential users of the payment system. As of now, countries are more likely to use alternative payment systems out of political necessity (e.g. seeking ways to transact via alternative payment systems like CIPS or SPFS to alleviate pressure from sanctions measures). Therefore, the payment system's efficiency and costs are not the main reason for participation from foreign users.

    However, an efficient and inexpensive payment system can limit the participation of U.S. payment companies. In the case of China, the Chinese government already limits the participation of U.S. payment companies as U.S. electronic payment services are denied market access. As people in the Chinese market increasingly adopts the eCNY, there will increasingly be less room for U.S. payment companies to potentially operate, even if restrictions of U.S. payment services are lifted. China intends to increasingly integrate the eCNY with Chinese domestic payment services, such as Tencent's WeChat Pay and Ant Group's Alipay. The PBOC will continue to herald eCNY integration, support its national champion China Union Pay, and exclude U.S. payment companies in the process.

15. U.S authorities and regulated financial institutions work together to collect data, identify suspicious financial activity, and prevent international money laundering. However, as more funds and transactions move away from the traditional banking architecture and into alternative payment systems, our conventional sanctions may become less effective.

    a. How can Congress and U.S. officials modernize our sanctions tools and be prepared to protect the international financial sector if a vast majority of transactions occur within the alternative payment ecosystem?

    There may be a future where a plurality of transactions could occur within the alternative payment ecosystem. As of now, what alternative payment systems such as CIPS and SPFS are processing (volume) are magnitudes lower compared to SWIFT's scale. However, it is crucial that the United States start deliberating possible policy options before potential crises come to fore.

    I have three policy recommendations. The first recommendation is analytic. I recommend concentrated government effort in monitoring the use, growth, and connectivity of all these alternative payment rails outside of the United States. For example, a signpost the U.S. government should watch out for would be whether more banks are starting to join the CIPS network, or whether Chinese and Russian alternative systems and rails are meaningfully collaborating. If so, there may be a critical mass of escape valves forming outside of the mainstream financial ecosystem. The Treasury Department should mandate an annual report on the use of the dollar in the context of global payment systems, which should also track the development of alternative payment systems.

    The second recommendation is defensive. The U.S. government should consider economic measures that could restrict the advancement of alternative payment rails. For example, if certain actors are trying to evade sanctions by facilitating transactions through CIPS, the Treasury Department should consider levying secondary sanctions on entities that helped with the transactions. Although before devising a sanctions program for this scenario, Treasury will need to study and anticipate to the extent it can the impact of such secondary sanctions prior to levying this tool, given potential unintended consequences from these measures.

    The third recommendation is proactive. I recommend concerted efforts from both the public and private sector in improving U.S. cross-border payment pipelines to make dollar transactions more efficient. Moreover, the United States needs to engage in standard setting bodies for digital assets and financial rails more proactively.

    In short, Congress and officials from relevant branches of the U.S. government must keep abreast of developments in the alternative payment ecosystem. Even though the status quo will not change in the short to medium terms, as US dollar dominance will ensure most actors want to be tapped into the mainstream financial system, it is prudent to have forward-leaning policy approaches as described above.

b. How can the U.S. engage with our international allies to defend against money launderers who exploit regulatory gaps in the alternative payment ecosystem?

At the present time, I have not conducted the necessary analysis to make assessments on how the U.S. can engage with international allies to defend against money launderers and other bad actors that exploit regulatory gaps in the alternative payment ecosystem. I echo the sentiment that multilateral coordination and action in monitoring alternative payment ecosystems is crucial to maintaining the integrity of the international financial system. I will investigate this important line of inquiry in future research.

16. The Treasury Department's 2021 Sanctions Review reported that, "technological innovations such as digital currencies, alternative payment platforms, and new ways of hiding cross-border transactions all potentially reduce the efficacy of American sanctions." It also recommended that Treasury dedicated more time and resources to understand digital asset services.

    a. In your opinion, do you believe that Congress, the Treasury Department, and law enforcement are prepared to position the U.S. to be a future leader in the global payment sector?

       The United States government has the capacity to ensure the United States maintains its leadership position in the global payments sector. Congress, the Treasury Department, and law enforcement all have crucial roles to play. Congress should ensure legislation targeted at monitoring other economies' payment systems and proactively investing in U.S. payments infrastructure are passed. The Treasury Department should allocate resources to monitoring current developments and projecting future trends. Law enforcement should monitor bad actors that may be transacting via alternative payment systems, and work with banks (institutions on the front line of sanctions compliance) to better address evasions of sanctions and the flow of illicit funds. As different parts of the U.S. government have varied roles, there should be a common set of objectives (perhaps in the form of a strategy document) to mobilize all stakeholders.

    b. What can Congress and U.S. officials learn from other countries' approach to appropriately monitor and regulate alternative payment systems?

       As countries are developing alternative payment systems, it is crucial that the U.S government understands their motivations, strategies, and desired end states. This kind of knowledge and analytical capability can empower the U.S. government in identifying significant trends and headwinds in the global financial system, and craft policy responses to safeguard the United States' economic and financial leadership for years to come.

Questions for the Record
Subcommittee on National Security, International Development, and Monetary Policy
Hearing entitled, "Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth"
Tuesday, September 20, 2022, at 10:00 a.m.

Witnesses

- Scott Dueweke, Global Fellow, Science and Technology Innovation, the Wilson Center
- Emily Jin, Research Assistant for the Energy, Economics and Security Program, the Center for a New American Security
- Dr. Carla Norrlöf, Nonresident Senior Fellow Economic Statecraft Initiative GeoEconomics Center, the Atlantic Council
- Ari Redbord, TRM Labs, Head of Legal and Government Affairs
- Jonathan Levin, Co-founder and Chief Strategy Officer, Chainalysis

1. Increased interoperability of alternative cross border payment systems could trigger a scenario where regional economies operate cross-border systems and settle transactions in currencies other than U.S. dollars, euros, or sterling. IMF Managing Director Kristalina Georgieva argues that this could create, "obstacles to the cross-border flow of capital, goods, services, ideas, and technologies."
    a. In your opinion, how could non-dollar denominated, regionalized payment systems affect U.S. regulators' ability to monitor cross-border flows?

If payment systems which are non-dollar denominated and regionalized become more prevalent, U.S. regulators' ability to monitor cross-border flows will decline.

    b. Could a system or series of systems like this help authoritarian regimes finance their efforts and evade traditional economic sanctions imposed by the U.S. and our allies?

Yes. When cross-border transactions are dollar denominated, they must eventually be cleared by a U.S. bank or financial institution, which face strict reporting requirements with regard to sanctions evasion and illicit finance. All other issuers of major currencies, apart from China, have strong incentives to comply with these measures since they often agree with the objective behind sanctions, and even when they do not, tend to comply in order to access the U.S. financial system. If cross-border transactions take place in the RMB or other minor currencies within a closed payments infrastructure which does not rely on SWIFT for communication, the payments would escape U.S. authorities, facilitating sanctions evasion and money laundering. The US may be able to leverage China's continued interest in accessing dollar-based payments systems and its interest in having US businesses and financial institutions use Chinese payments systems—in order to secure China's compliance with global financial standards.

2. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) network is the most widely used messaging system for cross-border payments between financial institutions. Following Russia's illegal invasion of Ukraine in February 2022, the European Unions, the United Kingdom, Canada, and the U.S. agreed to remove seven Russian banks from the SWIFT network.

a. What other cross-border payment mechanisms has Russia sought to replace the utility of the SWIFT network?

Russia reports that it is increasingly using its homegrown alternative to SWIFT, the System for Transfer of Financial Messages (SPFS), developed by Russia's central bank. Russia and China are using their respective currencies in their bilateral relations, and the Russian bank VTB has used RMB in its cross-border exchange with Chinese counterparts without relying on SWIFT. Russia is the second-largest oil exporter to India. Although they re-introduced the Cold War rupee-ruble mechanism shortly after Russia's invasion of Ukraine, bilateral trade imbalances and exchange rate volatility prevent them from transacting in each other's currencies. Dollars are used to settle Russian oil exports to India. Russia has attempted to promote the dirham, the United Arab Emirates' currency, for oil settlement between them. So far, Russian banks' requests for oil settlement in dirham have been declined by the correspondent bank in Dubai. Using dirham is attractive for Russians seeking to bypass the dollar because it provides the opportunity to recycle Russian wealth in Dubai where real estate and investment opportunities abound. Russia is also developing a blockchain platform for cross-border transfers using currencies and digital assets.

b. Have other countries looked to join alternatives to SWIFT in the wake of the sanctions imposed on Russia?

China is accepting RMB transfers from Russia outside of SWIFT. India is settling dollar payments to Russia outside of SWIFT. India has agreed to a joint rupee-ruble mechanism with Russia, independent of SWIFT, but it has been impractical due to exchange rate uncertainty. Russia's central bank claims that 50 new entities signed on to SPFS in 2022, totaling 440 users in total, a fraction of the SWIFT network's 11,000 users.

3. We have heard testimony today that widespread international adoption of these alternative payment systems is unlikely in the immediate future. The Russian ruble is volatile, and the Chinese government has imposed strict capital limitations on the RMB.

a. Why is the alternative payments ecosystem a potential threat to the U.S. and our allies?

While there are significant barriers in building alternative payments system due to the network externalities associated with the existing dollar-based payments system, there is a growing desire to operate outside the US dominated payments system. Countries hit by sanctions and countries who fear sanctions are taking steps to reduce their dependence on dollars. If China, Russia, India and Saudi Arabia were to realize an effective alternative to using dollars (and other allied currencies) for trade and investment, a substantial amount of economic activity including energy trade would occur outside the US centered financial system. These countries, particularly China, also have ties to other countries. By choice or necessity, their economic partners may start to gradually use the alternative payments systems adopted by their partners. If more and more countries move away from the dollar, the US will lose its geopolitical leverage to withhold access to the dollar system, freeze dollar accounts or reserves to pressure countries into compliance with international norms. US sanctioning powers will erode. The US will have less information about the cross-border transactions taking place, weakening its ability to combat money laundering. The dollar will remain the dominant currency in absolute terms but its relative dominance will be less pronounced. As a result, the advantages with dollar dominance will decline. Diminished dollar dominance in

this context implies a more multipolar currency world. Aside from the loss of US advantages, the use of multiple currencies, on a large scale, can be systematically destabilizing.

b. Is it only a threat if Russia and China build more robust global economic ties and volume?

More robust global economic ties and volume is needed in order for economic interactions and settlement within alternative payments systems to substantially affect the dollar's international role. Significant trade and investment between China, Russia and a few other big countries would have noticeable effects even if many countries do not participate in alternative payments systems, but the more countries participate, the bigger the effect. The consequences for the dollar's international role magnify if the RMB is used in transactions not involving China, since it implies a greater role for the RMB as an international currency. However, even if the RMB is not primarily used by countries other than China, more trade in home and partner currencies will diminish the international role of the dollar since it will be used less frequently by countries previously trading and investing in dollars. Besides the threat to dollar dominance, alternative payments also threaten the efficacy of sanctions and the fight against illicit finance flows. Strengthened global economic ties and volume are not required in order for such cross-border flows to escape US law enforcement.

4. In the past decade we have seen an increase in alternative payment systems. China introduced their Cross-Border Interbank Payment System and Russia developed their System for Transfer of Financial Messages (SPFS) and Mir to process payments.
   a. What are the economic benefits or costs of maintaining a robust alternative payment system?

China's CIPS (Cross-Border Interbank Payment System) and Russia's (SPFS) System for Transfer of Financial Messages are payments and communication vehicles for cross-border settlement with the two respective countries. The systems benefit entities trading and investing with them. To the extent that these alternatives offer a more decentralized and competitive financial system they may, like digital alternatives, promote efficiency in existing payment infrastructure. There are however large costs with not being able to detect flows within these alternative payments systems due to the possibility of financial evasion.

b. What is the relationship between a strengthening Chinese payment system and RMB internationalization?

Chinese currency internationalization requires cross-border use of the Chinese currency (RMB) between countries other than China. CIPS (Cross-Border Interbank Payment System) is one way for China to facilitate use of the RMB in cross-border exchange with China. As countries grow accustomed to using RMB for settlement with China, they are more likely to begin using RMB for settlement with each other. However, the development of CIPS is insufficient for Chinese currency internationalization. In order to supply an international currency on a significant scale, China must move to capital account convertibility so that its currency can be easily acquired and investment flow freely in and out of China. The Chinese government has been reluctant to take these steps due to concerns about the financial and social unrest it might cause. In order to increase the

international role of the RMB, China also needs to shift away from an export-led growth model to a liquidity provision model, exporting financial assets. And in order to offer the rest of the world RMB denominated financial assets on any significant scale, China must deepen and widen capital markets. To compete with the main international currencies, the dollar and the euro, China must also reassure foreign investors that their investments are safe. Foreigners must have some degree of faith in Chinese political institutions and property rights protections. In short, greater use of RMB is a prerequisite for currency internationalization, and CIPS helps expand trade and investment in RMB, but CIPS is not sufficient to promote the RMB.

China can also promote use of the RMB through digital payments alternatives, as with the e-CNY, China's CBDC (central bank digital currency) announced in 2016 and introduced for 2022 Olympics attendees including foreigners. When fully implemented, the e-CNY will function independently of other payment and financial messaging systems, both for financial institutions and private users. Instead of settling cross-border transactions using the dollar dominated CHIPS and SWIFT system, the Chinese CIPS or Russian SPFS—the Chinese central bank will mediate transactions in digital currency between users in China and users abroad. By promising cheaper, faster and safer transactions, a Chinese CBDC can speed up RMB internationalization. In the case of a Chinese CBDC, safety concerns will likely be balanced against privacy concerns since the Chinese central bank will be able to identify the parties to all transactions as well as the size of the transaction, reducing some users' enthusiasm for the e-CNY. While the Chinese central bank also will have similar information for transactions within CIPS, privacy concerns are more likely on the retail side. This ability to monitor transactions between China and the rest of the world facilitates RMB internationalization by offering the Chinese central bank the ability to monitor, and reject, transactions in order to mitigate destabilizing capital flows, partly alleviating concerns about capital account liberalization.

As with CIPS, the e-CNY will complicate US lawmaker's ability to monitor and enforce sanctions and illicit finance regulations. Differently from CIPS, the e-CNY will not need financial messaging services via SWIFT or any other external platform. This has important consequences for different forms of financial evasion since SWIFT provides US lawmakers with information about cross-border transactions. China will be able to evade sanctions and other financial regulations and transact with sanctioned entities as well as entities seeking to bypass financial regulations. The e-CNY has the potential to take financial evasion to another level because it creates a permissible environment for private users seeking to bypass sanctions and illicit finance regulations.

5. China introduced the Cross-Border Interbank Payment System in 2015 to more efficiently settle and clear RMB transactions. Today CIPS services 1,280 financial institutions across 103 countries.
    a. What are PRC's intentions in maintaining CIPS and other alternative financial plumbing, rails, and nodes?

China is clearly trying to internationalize its currency and create a payments system independent of Western infrastructure. Issuing an international currency is part of China's ambition to excel economically, and perhaps rival US economic power. The more China relies on settling cross-border trade and investment using an alternative ecosystem, the less vulnerable China becomes to threats denying access to Western vehicles for commerce and finance including threats to deny access to the dollar as medium of exchange. China's ambition is to create an economic hub around its payments arrangements in order to expand

its economic base and political influence, with a parachute capable of neutralizing Western financial coercion. Alternative payments are a feature of economic rivalry and great power competition.

b. How should the United States respond to these developments in the PRC?

The United States cannot prevent other states from building alternative payments system. But they can make US-based entities' participation in them, and China's continued participation in dollar-based systems conditional on compliance with global financial norms. They can also discourage growth in alternative payments systems by making their own infrastructure more attractive. To this end, the US should make clear that it will prevent US companies and banks from using Chinese payments systems, and suspend Chinese companies and banks from dollar-based payments systems, if China neglects to enforce compliance with global financial standards. By expanding and facilitating cross-border trade and investment denominated in US dollars with countries home to entities participating in CIPS, the United States can slow progress and potentially roll back progress with CIPS. The United States may also want to reconsider how it penalizes sanctions violation. For instance, BNP Paribas is one of the entities participating in CIPS, and has publicly supported Chinese alternatives to the dollar centered system. BNP Paribas was fined $8.9 billion and sentenced to a five-year probation for violating US sanctions and faced a full year ban on dollar clearance. While the size of the fine is the highest fine on an entity in sanctions history, the scope of Paribas' sanctions violation was extraordinary. BNP Paribas engaged in $30 billion worth of prohibited transactions according to US investigators. The severity of the sanction is not in dispute, and not for me to assess or judge. The specific penalty which locked a portion of BNP Paribas out of clearing dollars are however not in the United States' interest. By preventing a major bank of an allied country, who has assumed responsibility for sanctions violations, from clearing dollars—the United States forces adaptation to alternative payments systems. Instead, the US should consider creating a mechanism for determining whether the violating entity is likely to breach sanctions in the future or whether sufficient measures have been taken to prevent relapse. While disconnecting banks and other entities from dollar clearance is a potent deterrent for future violations, the US should consider not barring dollar transactions in cases where entities plead guilty to violating sanctions, accept the consequences of violating them, and implement credible measures to prevent future violations. To mitigate adverse selection, and counter any perception that sanctions violators are getting off "lightly", continued access to the dollar system should be granted on a case-by-case basis with the threat of prohibitively costly measures in the event of future violations.

6. Mobile wallet applications have consistently made up more than 40% of global e-commerce value and are projected to account for more than half of all transactions by 2025.

a. What is driving the growth of these alternative payment systems?

Phone-based payment solutions are growing rapidly though there are significant differences across countries. Customer demand for more secure, convenient, faster, contact-less payment methods are driving growth in mobile wallets. Safety, convenience and cost-savings are primary benefits. By avoiding cash, mobile wallet users reduce the risk of physical harm often associated with hold-ups for cash. Encryption tends to make mobile wallet payments safer than credit card payments. The possibility of peer-to-peer payments adds convenience to phone-based payments. Increased online

presence during the Covid-19 pandemic was an obvious driver for the expansion of this payment method. But interest in FinTech (financial technology) preceded the pandemic and is likely to continue accelerating beyond the pandemic. By cutting out financial intermediation, these wallets allow users to receive, send and store money on a mobile phone and use other financial services without costly bank accounts, broadening financial inclusion.

b. These systems can pose greater threats when they grow in size and volume, and when they might become interoperable. What are some of the issues that would require a U.S. and allied response?

Despite the promise of reduced risks to physical theft and harm from avoiding cash and credit card payments, mobile wallets introduce security risks which require monitoring and allied cooperation.

7. Non-U.S. mobile payment applications reportedly reach more than 1 billion consumers and process over $60 trillion worth of transactions worldwide. Continued advancement of these products into foreign markets can diminish U.S. competitiveness and yield opportunities for foreign governments to influence international payment principles.

a. How can Congress help promote and encourage participation of U.S.-based payment companies in foreign markets?

The reported dollar worth of non-U.S. "mobile" payment transactions is significantly less than the quoted number above. Nevertheless, Congress has a role to play because the US ranks as the second largest mobile payments market after China, and accounts for roughly a third of China's transactions. Congress can support U.S.-based mobile payment companies in foreign markets by encouraging both providers and merchants to create network externalities. In order to tap into foreign markets, foreign users must be offered the opportunity to access many merchants. Investing in multiple mobile payment applications is expensive for merchants. By reducing fragmentation in the US market, incentivizing interoperable mobile payments applications, merchants would only have to bear the cost of investing in one, or a few, platforms while reaping the potential benefits of purchases from many customers. The biggest mobile payments providers are likely to resist removing such barriers to entry unless they are able to see that the potential profits from extending use of the mobile payment application exceed profits from the extra devices sold with mobile payment services. Mobile payments applications should also be interoperable with foreign applications, allowing foreigners to access US merchants and for US residents to make payments to foreigners. Congress can play a role by ensuring competitiveness, safety and privacy requirements are met as providers and merchants seek to raise network effects for mobile payments.

b. What regulatory standards should policymakers consider to ensure that U.S. companies remain competitive in the international payment sector?

8. The growth and expansion of alternative cross-border payment systems could lead to a world less dependent on U.S. dollars, which would likely limit our traditional methods of economic sanctions.

a. How should U.S. national security experts be preparing our sanctions toolkit to respond to this scenario?

Whenever possible, the United States should work with like-minded countries, especially other countries issuing currency majors, to determine whether and to what extent sanctions should be imposed by a coalition of countries. The greater the number of currency major countries participating in the sanction effort, the fewer alternative currencies there are to replace dollar settlement. Such a strategy will complicate the use of viable alternatives to the dollar, though they will hasten use of upcoming alternatives to the principal currency majors, notably the RMB. To mitigate this effect, the United States and allies should incentivize settlement in currency majors. The United States could for instance tie economic inducements to promises from beneficiaries to settle cross-border exchange with third parties in dollars. Even if countries are unable to resist Chinese or Russian demands to settle trade in RMB or ruble respectively, trade not involving them would continue to be priced in dollars (or other currency majors). Placing a ceiling on cross-border settlement in RMB and ruble, will limit China's ability to internationalize its currency.

b. What are some examples of nonfinancial sanctions measures that could act as a deterrent in the same way that financial sanctions do today?

Export and import controls can be effective instruments of coercion if properly calibrated. Export controls can be applied to deny firms access to vital inputs including technology. Import controls can be used to deny firms access to the US market. Trade restrictions are however more cumbersome to use than financial sanctions and a less potent instrument of coercion unless the targeted entity or country in question is highly dependent on the United States.

9. Sanctions that are made possible because of the strength of the U.S. dollar could push countries to reduce their use of U.S. dollars and minimize the global economic power of the United States. Although the dollar will likely be the world's primary reserve currency for the foreseeable future, governments could experiment with other national currencies to proactively shield their economies from the U.S.
    a. How long could a government successfully sustain itself without using currencies like dollars, euros, or sterling?

How long a country could operate without access to dollars, euros and sterling, depends on the country's dependency on the above-mentioned currency majors and the alternative currencies available for transaction purposes including the viability of the home currency. Any country's resilience will depend on how extensive the country's economic ties are to the United States, the euro zone and the United Kingdom. The greater the significance of the country's trade and investment in these locations, the more dollars, euros and sterling, as well as dollar, euro and sterling denominated assets, it will need to acquire.

b. What inflection points would signal that major economies are attempting to de- dollarize? How should U.S. policymakers address that scenario?

If major economies shift their trade and investment relations away from the United States, they will have less need for US dollars, and could choose to reduce dollar denominated settlement with other countries. However, while such changes "could" reduce aggregate dollar holdings, the effect need not be dramatic since the United States has sustained dollar dominance despite a lower, and shrinking, role in world trade. To the extent possible, the US should track growth in the number of private entities and countries participating in alternative payments systems. This may for instance be easier with respect to China and India's platforms than with Russia's. A second related development to track is private use of dollars. If the actors and agents engaging in cross-border trade and investment reduce their use and exposure to dollars, a de facto shift in the dollar's global role will have taken place, requiring governments to hold less dollars. Gauging the use of dollars as a borrowing vehicle could also be a way of identifying whether important changes are taking place, and whether the dollar's appeal is fading for businesses and financial institutions. Third, short of gradual increases in the portion of reserves held in other currencies, swap agreements with other currency issuers, notably China, is yet another indication that major countries are making contingencies for reduced dollar holdings.

10. In April, the Russian Minister of Finance proposed that Brazil, Russia, India, China and South Africa integrate their payment systems to promote greater use of Mir and domestic currencies in cross-border financing.

    a. Do you believe this is likely to happen?

The BRICS are integrating their payments systems to facilitate cross-border exchange and promote national currencies and local payment alternatives. For example, China and Russia have issued a UnionPay-Mir debit card, though China has limited cooperation with sanctioned Russian banks due to fears of US secondary sanctions. UnionPay stopped issuing cards to Russian banks under sanctions following Russia's 2022 invasion of Ukraine. India and Russia have created a rupee-ruble mechanism to settle cross-border exchange between them, though the initiative has been stalled due to exchange rate volatility. India and Russia have also been exploring ways for India to tap into the Mir payment system. Before the United States sanctioned the CEO of Russia's NSPK (National Card Payment System) which operates Mir, roughly a dozen countries were using Mir and another dozen had expressed interest in joining. Most countries are likely to postpone adoption of Mir, and halt existing plans, following threats of secondary sanctions from OFAC (Office of Foreign Assets Control) if firms and banks use Mir. Six countries, Armenia, Kazakhstan, Tajikistan, Uzbekistan and Turkey, all suspended their participation in Mir after the US Treasury's warning. The BRICS countries have also explored issuing a joint reserve currency, with the explicit purpose of bypassing the dollar and other Western currency majors. A collective reserve currency is fraught with problems and unlikely to be successful. Greater use of their national currencies, as well as greater use of the Chinese RMB, is more likely.

    b. How would this mitigate the impact of Ukraine-related economic and trade sanctions?

Concerns about secondary sanctions complicate Russia's sanctions evasion. China suspended UnionPay cards for sanctioned banks in Russia. Non-sanctioned Russian entities are however able to open accounts with UnionPay. Outside BRICS, Kazakhstan provided Russians with access to virtual VISA and Mastercards to facilitate payments in dollars and euros. Turkey's suspension of Mir is particularly significant since Russia was

able to circumvent sanctions by using Mir to make and receive payments to European firms via Turkey.

11. One of the benefits of the SWIFT network is that SWIFT messages are standardized, secure, and relatively inexpensive, helping connect 11,000 financial institutions across more than 200 countries. However, competing cross-border messaging and clearing systems may challenge SWIFT's leadership, complicate international finance, and make it difficult for U.S. regulators to track illicit flows.

    a. How complicated is it to create a network that is similar and comparable to SWIFT?

Creating an efficient and secure financial communication system rivaling SWIFT will be challenging. Even if another company or cooperative leverages the technology to create a SWIFT-like platform for secure financial messaging, any shift away from SWIFT is likely to be incremental and unlikely to replicate the size of the SWIFT network. The benefits of using SWIFT come down to the unsurpassed scale of the SWIFT network, which alternative platforms are unlikely to reproduce, not least because there are different contenders trying to replace SWIFT. China offers CIPS (Cross-Border Interbank Payment System) and may make their financial messaging independent from SWIFT. Russia offers SPFS (System for Transfer of Financial Messages). India intends to connect UPI (Unified Payment Interface) to other countries and is touting the platform as a potential alternative to SWIFT. Interoperability challenges makes this an unlikely near-term development on any substantial scale. Attractive features of India's UPI are their low-cost and real-time payment features, which SWIFT is trying to mimic, though instantaneous payments are more difficult to secure.

While Western sanctions, in this case, the removal of Russian entities from SWIFT, has prompted countries to discuss SWIFT alternatives, other countries also face geopolitical barriers to cooperation. For example, privacy concerns pose a challenge for BRICS countries, particularly China and India, when connecting payments systems.

    b. Should we anticipate that a major competitor to SWIFT could be developed in the near future, and if so, how should national security and financial intelligence professionals prepare for that shift?

A major competitor to SWIFT is highly unlikely to emerge in the near future. National security and financial intelligence officers should nonetheless prepare for greater use of alternative payments systems since we are likely to see a more fragmented system over time even if a single competitor is unlikely to rival SWIFT. With more transactions taking place outside of SWIFT, the US will lose information about transactions it is currently able to access over SWIFT, and will therefore lose a valuable monitoring tool for financial evasion. In addition to losing information about which transactions are made, alternative platforms are likely to have lower financial standards, posing a challenge for law enforcement. The primary risks with these lower standards are sanctions evasion, money laundering and privacy breeches. While, for instance, China has updated regulations aimed at improving AML (anti-money laundering) compliance, comprehensive AML and KYC (Know-Your-Customer) rules have not been implemented. US national security and financial intelligence

professionals will not have access to information about cross-border transactions within CIPS, SPFS or UPI unless Chinese, Russian or Indian officials voluntarily share the data. If US officers suspect sanctions evasion or illicit finance within these networks, they will need alternative intelligence gathering methods to uncover such violations.

12. In 2014, Russia began developing its own financial messaging and banking card systems after the U.S. imposed strict sanctions in response to Russia's illegal annexation of the Crimean Peninsula. These systems allow Russia to continue processing domestic payments, though cross-border options. They also allow access to currencies widely used in international transactions that are limited due to the sanctions imposed by the U.S. and allies after Russia's illegal invasion of Ukraine in February 2022.

    a. How have Russia's financial messaging and banking card systems helped insulate its economy from sanctions?

This is a difficult question to answer due to the opacity of the SPFS network. In order to insulate participating businesses, banks and countries from US secondary sanctions, the Russian Central Bank will not disclose who uses SPFS. While some countries have deferred Mir participation for fear of secondary sanctions, it is unclear whether SPFS users have disconnected from the system given the significantly lower risk of detection. Before OFAC threatened secondary sanctions against entities helping Russia bypass sanctions through Mir, Turkey facilitated significant transactions between Russia and Europe. Similarly, Kazakhstan enabled dollar and euro payments through virtual credit cards before interrupting services under the weight of OFAC threats. Since these suspensions only occurred in September, Russia would have benefited from the Mir workarounds for some 6 months.

    b. What is the likelihood that other countries may look to replicate Russia's payment system strategy to defend their economy from economic sanctions?

Countries planning to violate norms that invite sanctions are likely to prepare back-channels to settle payments. Certainly, China has considered the possibility of being shut out of the dollar system given its objective to reunify with Taiwan and the United States' commitment to defend Taiwan. But most countries bear no resemblance to Russia, an authoritarian great power fueled by energy and territorial nostalgia. It is hard to think that other countries look at where Russia is now and come to the conclusion that they want to emulate its self-inflicted military blow, hollowed economic power and loss of cultural cachet. As long as the US is clear that the nature of the sanctions on Russia matched the severity of Russia's norm violation, countries are unlikely to fear the same punishing sanctions, and less likely to build alternatives payment systems. Moreover, Russia, China and India differ from most other countries in that three of them have the scale to make homegrown payments alternatives worthwhile. Russia and China are great powers. India is a potential great power. That is not true of most countries who are more likely to tap into existing payments systems than to develop their own systems.

13. Many alternative payment systems are domiciled or operating in nations with antimony laundering standards that are not as strict as those proposed by the Financial Action Task Force and U.S. law and regulations. This means that in many cases, transactions are processed without any attempt by the operator to know the customers on each end of the transactions.

The result is that financial crime, including money laundering and sanctions evasion, can occur in plain sight.

a. Are know your customer (KYC) checks effective for these alternative payment systems?

China has updated regulations aimed at improving AML (anti-money laundering) compliance, but comprehensive AML and KYC (Know-Your-Customer) rules have not been implemented. India has KYC checks, but unlikely as robust as SWIFT verification. The Bank of Russia has developed its own KYC platform.

b. Do they need to be implemented in all systems, why or why not, and what are examples of where such standards could be useful to America's national security interests?

The KYC framework can be useful tool to track sanctions evasion and illicit finance. KYC is however insufficient to ensure compliance with global financial standards if supervisors within alternative payments systems are able to influence KYC triggers.

14. Some national security experts predict that authoritarian governments will leverage digital payment infrastructure and central bank digital currencies as a tool for economic coercion and global data surveillance.

a. How do alternative payment rails play a role in countries' political and economic strategies?

Promoting alternative payments systems are a means for shifting the balance of power within the current order and realizing an alternative international order. Reducing dollar dominance reduces US economic and geopolitical power. Alternative payments systems are a stepping stone towards currency internationalization for China, and over the longer term possibly for India. Issuing an international currency is associated with economic power, geopolitical power, and prestige. China is a great power and potential rival to US primacy; India is a potential great power. Russia is a great power though its economic base is more narrowly grounded in raw materials; Russia has supported China's international currency ambitions but not expressed any of its own. Alternative payments are also a form of insurance against Western financial coercion.

If alternative payments are successfully implemented with broad-based participation, the US can expect its role to diminish in a number of key respects. We are likely to see a decline in US benefits from international economic engagement. US seignorage and monetary flexibility will decline. The US government's centrality in international monetary relations, and the centrality of US financial institutions within the international economy is also likely to diminish. A less prominent role for the dollar, the US government and US financial institutions in international monetary relations and finance could also make the US more susceptible to crises originating elsewhere, and without the safe haven benefits of issuing the global currency. If these disadvantages cumulate, they could propel relative economic decline, which could pose problems for America's ability to fund its military edge.

The United States' ability to effectively sanction other countries, and entities within countries, will be curtailed if the dollar, CHIPS and SWIFT system become less prominent. Withholding access to dollars will be less effective as a broad-based policing mechanism if fewer official and private actors transact in dollars, hold dollar accounts and participate over dollar dominated platforms. Declining dollar dominance (and Western currency dominance) raises the risk of increased sanctions evasion and other forms of financial evasion, eroding a non-military tool to enforce norms ranging from human rights to democracy to peaceful international relations.

b. Can an efficient and inexpensive payment system be a soft power tool and further limit participation of U.S. payment companies?

15. U.S authorities and regulated financial institutions work together to collect data, identify suspicious financial activity, and prevent international money laundering. However, as more funds and transactions move away from the traditional banking architecture and into alternative payment systems, our conventional sanctions may become less effective.

a. How can Congress and U.S. officials modernize our sanctions tools and be prepared to protect the international financial sector if a vast majority of transactions occur within the alternative payment ecosystem?

It is highly unlikely that a vast majority of transactions will migrate to alternative payment ecosystem any time in the near or medium-term. A larger portion of transactions is however likely to occur within alternative payments structures. To the extent possible, the US should aim to make these systems coexist with enforceable standards for illicit finance, sanctions and tax evasion even if they require unilateral enforcement or enforcement by a small coalition. China and India, and likely Russia after war's end, will want to continue participating in CHIPS and SWIFT in spite of their parallel efforts to advance their respective payments systems. US and European businesses and banks will also want to access alternative payments systems, to some extent. If alternative payments systems become feeding ground for money laundering and serve as sanctions havens, US and European regulators can threaten to unplug private and official actors offering payment loopholes. They can also threaten to prevent their own businesses and banks from participating in foreign payments systems. The larger the group of countries enforcing these standards, the greater the likelihood of success.

b. How can the U.S. engage with our international allies to defend against money launderers who exploit regulatory gaps in the alternative payment ecosystem?

16. The Treasury Department's 2021 Sanctions Review reported that, "technological innovations such as digital currencies, alternative payment platforms, and new ways of hiding cross-border transactions all potentially reduce the efficacy of American sanctions." It also recommended that Treasury dedicated more time and resources to understand digital asset services.

a. In your opinion, do you believe that Congress, the Treasury Department, and law enforcement are prepared to position the U.S. to be a future leader in the global payment sector?

The US is likely to continue playing the lead role in global payments for the foreseeable future. Dollar dominance, the existing CHIPS (Clearing House Interbank Payments System) network and dominance within the SWIFT network make the US well-positioned to compete in the financial and currency system. However, CBDCs (central bank digital currencies) and alternative payment systems challenge US sanctioning powers because the informational advantage shifts from the US government to foreign governments. Making access to Western payments systems, and Western entities' access to non-Western payments systems, conditional on compliance with global financial standards is one source of leverage. The US should continue to monitor growth in the participating countries and entities within payments networks and the various steps taken towards interoperability of different payments systems.

b. What can Congress and U.S. officials learn from other countries' approach to appropriately monitor and regulate alternative payment systems?

TRM

Questions for the Record
Subcommittee on National Security, International Development, and Monetary Policy
Hearing entitled, "Under the Radar: Alternative Payment Systems and the National Security Impacts of Their Growth"
Tuesday, September 20, 2022, at 10:00 a.m.

November 10, 2022

Increased interoperability of alternative cross border payment systems could trigger a scenario where regional economies operate cross-border systems and settle transactions in currencies other than U.S. dollars, euros, or sterling. IMF Managing Director Kristalina Georgieva argues that this could create, "obstacles to the cross-border flow of capital, goods, services, ideas, and technologies."

a. In your opinion, how could non-dollar denominated, regionalized payment systems affect U.S. regulators' ability to monitor cross-border flows?

b. Could a system or series of systems like this help authoritarian regimes finance their efforts and evade traditional economic sanctions imposed by the U.S. and our allies?

Focusing on the use of cryptocurrencies as the "alternative cross border payment system," digital assets and blockchain based technologies allow for the more efficient and effective combating of financial crime and enable U.S. regulators to monitor cross-border flows with unprecedented visibility. The native properties of public blockchains — data that is Transparent, Traceable, Public, Permanent, Private, and Programmable — enable compliance professionals, law enforcement, regulators, supervisors, and other government agency officials to more readily identify, investigate and mitigate financial crime risks. Blockchain intelligence tools are a key part of this, enabling entities to exploit these inherent characteristics.

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.

TRM

The transparency of blockchain-based transactions provides visibility into illicit transaction volume that would otherwise be unattainable. 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 - a fact that is only obtainable because of the transparent nature of the blockchain.

Traceable

For government investigators, it can take months or even years to follow the trail of a sophisticated criminal, oftentimes requiring subpoenas across multiple service providers in various jurisdictions and necessitating that law enforcement 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 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. 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 incoming deposits of proceeds from a ransomware attack, even if the funds moved through multiple transactions before being deposited.

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.

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.

Programmable

The unique qualities of blockchains allow for enhanced regulatory oversight. The BSA framework currently requires banks and other Money Service Businesses ("MSBs") to register with FinCEN, to maintain an AML program, and to file suspicious activity reports ("SARs") when suspicious activity arises. This means that FinCEN must rely on intermediary financial institutions, with oversight only over the transactions they directly administer, to identify risky behaviors and to submit a report that is actionable and valuable to law enforcement officials.

Blockchain technology has the potential to disrupt the siloed, end-user generated, one-way communication of SARs. Depending on the circumstances, a transaction could even be blocked, or held in escrow, before it is carried out based on identity information provided by regulators.

Regulators are not restricted to accessing only transaction data, but could also access profiles on digital entities, custodians, and stablecoin issuers, among others. Oversight can be conducted across multiple blockchains, revealing the percentage of trade linked to high-risk activities. Collection of data directly from the blockchain is precisely the sort of risk- based and agile regulatory practice that would increase efficiency and effectiveness for managing financial crime risk.

In October 2021, the Financial Action Task Force ("FATF") issued guidance encouraging regulators to use blockchain intelligence to identify persons operating without a license or registration. It further recommended enhanced due diligence with respect to certain virtual asset service providers, including those engaged in cross-border correspondent relationships, leading to more effective implementation of risk-based controls. FATF highlights the fact that certain jurisdictions, including the United States, already use blockchain analytics in their supervision of regulated entities.

A revised regulatory approach using blockchain intelligence would benefit both regulators and digital asset providers. The availability of raw blockchain data, unprecedented both in quantity and quality, gives regulators the ability to instantly access relevant information across borders without the lag time or filtering mechanism inherent in relying on intermediaries to submit SARs.

TRM

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) network is the most widely used messaging system for cross-border payments between financial institutions. Following Russia's illegal invasion of Ukraine in February 2022, the European Unions, the United Kingdom, Canada, and the U.S. agreed to remove seven Russian banks from the SWIFT network.

a. What other cross-border payment mechanisms has Russia sought to replace the utility of the SWIFT network?

b. Have other countries looked to join alternatives to SWIFT in the wake of the sanctions imposed on Russia?

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 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.

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), the MIR domestic payments system, and in September 2022, 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. Similarly, in August, Iran made its first official import order – worth $10 million, according to reports – using cryptocurrency, in a move intended to evade U.S. sanctions.

We are not just talking about adversaries. Allies in Europe and the United Kingdom have called for an international currency to "dampen the domineering influence of the U.S. dollar on global trade." 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.

TRM

We have heard testimony today that widespread international adoption of these alternative payment systems is unlikely in the immediate future. The Russian ruble is volatile, and the Chinese government has imposed strict capital limitations on the RMB.

a. Why is the alternative payments ecosystem a potential threat to the U.S. and our allies?

b. Is it only a threat if Russia and China build more robust global economic ties and volume?

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. 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 Development of Digital Assets (executive order), prioritize principles of privacy, security, and "the ability to exercise human rights," in this new financial system?

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.

TRM

Non-U.S. mobile payment applications reportedly reach more than 1 billion consumers and process over $60 trillion worth of transactions worldwide. Continued advancement of these products into foreign markets can diminish U.S. competitiveness and yield opportunities for foreign governments to influence international payment principles.

a. How can Congress help promote and encourage participation of U.S.-based payment companies in foreign markets?

b. What regulatory standards should policymakers consider to ensure that U.S. companies remain competitive in the international payment sector?

When focusing on the digital asset ecosystem, Congress can help promote and encourage the growing regulated dollar-backed stablecoin ecosystem. 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.

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, principle based and outcome driven 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.

The growth and expansion of alternative cross-border payment systems could lead to a world less dependent on U.S. dollars, which would likely limit our traditional methods of economic sanctions.

a. How should U.S. national security experts be preparing our sanctions toolkit to respond to this scenario?

b. What are some examples of nonfinancial sanctions measures that could act as a deterrent in the same way that financial sanctions do today?

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.

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.

TRM

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. 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.

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.

Many alternative payment systems are domiciled or operating in nations with anti-money laundering standards that are not as strict as those proposed by the Financial Action Task Force and U.S. law and regulations. This means that in many cases, transactions are processed without any attempt by the operator to know the customers on each end of the transactions. The result is that financial crime, including money laundering and sanctions evasion, can occur in plain sight.

a. Are know your customer (KYC) checks effective for these alternative payment systems?

b. Do they need to be implemented in all systems, why or why not, and what are examples of where such standards could be useful to America's national security interests?

In the digital assets space, the implementation of FATF's standards is critical to mitigate the risks of money laundering. The entire ecosystem is only as strong as its weakest link as jurisdictional arbitrage continues to be a challenge in the wake of inconsistent global regulatory frameworks. For example, according to TRM Labs analysis, Russia has the largest percentage of high-risk virtual asset service providers (VASPs). After the invasion of Ukraine TRM identified approximately 340 Russia based VASPs that could be used to launder funds due to weak or non-existent KYC controls. These non-compliant Russia based VASPs have been a target for OFAC which has designated three such exchanges – SUEX, Chatex and Garantex.

But we are also seeing compliant VASPs in the U.S. and elsewhere build sophisticated and effective compliance controls including the use of KYC and blockchain intelligence tools. Some jurisdictions, such as New York's Department of Financial Services, are even requiring the use of such tools for licensed entities.

TRM

Some national security experts predict that authoritarian governments will leverage digital payment infrastructure and central bank digital currencies as a tool for economic coercion and global data surveillance.

a. How do alternative payment rails play a role in countries' political and economic strategies?

b. Can an efficient and inexpensive payment system be a soft power tool and further limit participation of U.S. payment companies?

Economic controls have historically played a key role as authoritarian regimes attempt to gain leverage and control over their citizens. Authoritarian regimes seek to control the means and methods of commerce in order to exert control over their population. But, the promise of digital assets – decentralized cross border value transfer at the speed of the internet – also enables average citizens, dissidents, and marginalized people to send funds outside of the traditional financial system in order to maximize privacy and thwart surveillance. We have seen this play out in places like Ukraine where people have sent millions of dollars of aid in cryptocurrency outside of traditional channels.

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. The balance that policy makers need to strike is to protect national security while also preserving the privacy of regular users who seek, not anonymity, but a degree of privacy in a more open financial system.

It bears noting that privacy can be enabled in a way that is compliant with our AML/CFT/CPF regime and ensures democratic principles. 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.

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.

U.S authorities and regulated financial institutions work together to collect data, identify suspicious financial activity, and prevent international money laundering. However, as more funds and transactions move away from the traditional banking architecture and into alternative payment systems, our conventional sanctions may become less effective.

a. How can Congress and U.S. officials modernize our sanctions tools and be prepared to protect the international financial sector if a vast majority of transactions occur within the alternative payment ecosystem?

b. How can the U.S. engage with our international allies to defend against money launderers who exploit regulatory gaps in the alternative payment ecosystem?

As set forth above, in a blockchain-based economy, sanctions are still a powerful tool and can be used as both a punitive measure and as a deterrent. We have seen regulators utilize the unique qualities of blockchains to deploy sanctions and bring enforcement actions for non-compliance. For example, we have seen OFAC sanction non-compliant Russia-based VASPs SUEX, Chatex and Garantex, darknet markets like Hydra, and mixers like blender.io and Tornado Cash. In addition we have seen OFAC and FinCEN bring enforcement actions against crypto businesses such as Bitgo, Bitpay and Bittrex that did not have the necessary blockchain intelligence and geolocation tools in place to block transactions with sanctioned jurisdictions such as Sudan, Iran, North Korea, Syria and others.

The unique qualities of blockchains married with blockchain intelligence tools allow regulators more visibility on financial flows than they have in the traditional financial system. Ensuring that the right tools and training are deployed across law enforcement and regulators in the U.S. and globally is critical to modernizing, enforcing and maintaining the efficacy of the sanctions regime.

TRM

The Treasury Department's 2021 Sanctions Review reported that, "technological innovations such as digital currencies, alternative payment platforms, and new ways of hiding cross-border transactions all potentially reduce the efficacy of American sanctions." It also recommended that Treasury dedicated more time and resources to understand digital asset services.

a. In your opinion, do you believe that Congress, the Treasury Department, and law enforcement are prepared to position the U.S. to be a future leader in the global payment sector?

b. What can Congress and U.S. officials learn from other countries' approach to appropriately monitor and regulate alternative payment systems?

Please see TRM Labs' response to Treasury's request for comment on "Ensuring Responsible Development of Digital Assets" here: https://www.trmlabs.com/post/ensuring-responsible-development-of-digital-assets-request-for-comment

In addition, we have seen the Department of Justice (DOJ), F.B.I., Homeland Security Investigations (HSI), IRS-Criminal Investigations (IRS-CI), United States Secret Service and other law enforcement agencies build the capacity to investigate and prosecute cryptocurrency-related fraud and financial crime. We have seen the establishment of the National Cryptocurrency Enforcement Team (NCET) at DOJ, the Virtual Asset Unit (VAU) at F.B.I. and myriad other specialized squads across the interagency. We have seen an increase in the investigation of crypto-related fraud and financial crime. Here are a few things Congress can do to continue to support these efforts:

- Ensure that policymakers, regulators, supervisors and law enforcement have the necessary training and tools to effectively identify and mitigate illicit finance risk in digital assets. While it is possible to enhance the current regulatory and supervisory practices by utilizing blockchain intelligence tools, it is paramount that these tools, and training, be made readily available to regulators and investigators both in the U.S. and, to the extent possible, in jurisdictions that can benefit from capacity building.

TRM

- **Enhance public private partnerships (PPPs)** with real time information exchange to equip the private sector with the data they need to combat financial crime and the information supervisors need to conduct real time supervision. For PPPs to be effective it is essential that a broad range of stakeholders are included and participate. The United States Treasury should map the digital asset ecosystem to ensure that it includes a good representation of the industry in its PPPs and review information sharing mechanisms to ensure that they are fit for purpose in the digital asset age. Finally, criminals who exploit digital assets are based across the world, to create an international response to this problem domestic PPPs should aspire to collaborate with PPPs in allied nations.

- **Uplift cybersecurity expectations and capabilities** across the industry to make it more difficult to attack the digital asset infrastructure and profit from malicious activity. Users must be upskilled in cybersecurity practices for the digital asset ecosystem. The private sector who operate in the digital asset space should have processes in place to respond to cybersecurity events when they occur including incident response and when attacks do occur, government agencies should be able to share appropriate information on them with blockchain intelligence firms to help stop future attacks.