TESTIMONY OF

Jane Khodarkovsky

BEFORE THE

U.S. House Financial Services Committee, Subcommittee on Digital Assets, Financial Technology and Inclusion

"Crypto Crime in Context: Breaking Down the Illicit Activity in Digital Assets"

November 15, 2023

INTRODUCTION

I am honored to speak with you today and grateful to be able to contribute to what I believe is the unique challenge to preserving the United States' ideals and values. In 1992, when I was a child, my family and I left Odesa, Ukraine, then part of the former Soviet Union, as refugees. I sit before you the product of the United States' leadership in innovation and promotion of democratic ideals while countering illicit finance and autocratic regimes. Today, more than ever before, those ideals and commitments are being challenged around the world, and we are at a critical juncture to safeguard those ideals and the country's national security.

As a Trial Attorney and Human Trafficking Finance Specialist in the Money Laundering and Asset Recovery Section of the U.S. Department of Justice (DOJ), and previously as a local and state prosecutor, I investigated and prosecuted financial crimes, including money laundering and corruption. Following the money to detect, dismantle, and disrupt those who disguise, conceal, and attempt to obfuscate the U.S.'s financial system to commit crimes, including funding terrorism or authoritarian leaders, was critical. My former colleagues, law enforcement partners, and the whole of government (including other federal agencies, such as the Financial Crimes Enforcement Network (FinCEN), Office of Foreign Assets Control (OFAC), Internal Revenue Service (IRS), etc.) worked to identify not only those directly engaging in criminal activity but also those who were acting as "gatekeepers" or third-party facilitators like bankers, real estate agents, and lawyers, to help facilitate and conceal those crimes. It was critical to conduct financial investigations in parallel to the investigations of the underlying criminal activity, whether human trafficking, child exploitation, terrorist financing, and other financial crimes, to ensure that real property and assets that were proceeds of, facilitated, or were involved in the criminal network could be seized and forfeited.

I am often asked why I transitioned from DOJ to the private sector to work and support software developers in the blockchain space. The answer is quite simple - I believe that this technology, which is open, transparent, immutable, and can be accessed by people of all backgrounds around the world, is critical to the future. And, technology is not inherently good or bad. It is how the technology is used that must be evaluated and addressed. We live in a world where innovation is moving rapidly, including changing how people and companies interact with the new technology and its applications. As a particular technology – and the way

in which it is used – evolves, so too should the risk based analysis of whether the legislative, regulatory and legal frameworks need to follow. I believe that we cannot promote innovation without also protecting consumers and combating illicit finance and terrorist financing. We must do so with circumspection and nuance.

The 2020 DOJ Report of the Attorney General's Cyber Digital Asset Task Force stated that there were over 2,000 cryptocurrencies used to transfer value around the globe in exchange for goods, services, and other sources of value.[1] As of 2022, data from Chainalysis suggests that the percentage of all cryptocurrency activity associated with illicit activity was 0.24%.[2] While all statistics should be evaluated in context, there is little verifiable comparison between the percentage of illicit activity through traditional financial systems given the lack of an immutable public ledger.

Importantly, in my experience, sophisticated criminal actors who engage in money laundering and terrorist finance leverage all available financial instruments and methods to further their criminal activity and often do not do so in silos. This is evident in the below DOJ cases.

After the Russian invasion of Ukraine on February 22, 2022, DOJ launched the Kleptocapture Taskforce.[3] The taskforce specifically targets criminal actors—regardless of whatever means of exchange they use—to defend and protect the U.S. economy from illicit funds linked to Russia. As of March 2023, thirty-five individuals and corporations were charged.[4] The assets seized in the United States and abroad included at least four yachts[5] whose

---

1 U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework* (October 2020), at 5, https://www.justice.gov/archives/ag/page/file/1326061/download#:~:text=As%20the%20Task%20Force%20has,crimes%2C%20such%20as%20theft%2C%20directly (herein referred to as "2020 Crypto Enforcement Framework").

2 Chainalysis, *The 2023 Crypto Crime Report* (February 2023), at 6, https://go.chainalysis.com/2023-crypto-crime-report.html.

3 Press Release, U.S. Department of Justice, Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture (March 2, 2022), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.

4 Ryan Lucas, *Over the Past Year DOJ's Task Force Kleptocapture Has Been Extremely Busy*, NPR Illinois (March 3, 2023), https://www.nprillinois.org/2023-03-03/over-the-past-year-dojs-task-force-kleptocapture-has-been-extremely-busy.

5 *See, e.g.*, Press Release, U.S. Department of Justice, $300 Million Yacht of Sanctioned Russian Oligarch Suleiman Kerimov Seized by Fiji at Request of United States (May 5, 2022), https://www.justice.gov/opa/pr/300-million-yacht-sanctioned-russian-oligarch-suleiman-kerimov-seized-fiji-request-united; Press Release, U.S. Department of Justice, $90 Million Yacht of Sanctioned Russian Oligarch Viktor Vekselberg Seized by Spain at Request of United States (April 4, 2022), https://www.justice.gov/opa/pr/90-million-yacht-sanctioned-russian-oligarch-viktor-vekselberg-seized-spain-request-united; Tal Yellin, *From Yachts to Lavish Estates, Tracking Russian Assets Seized So Far*, CNN

combined value was just under $1 billion dollars, six real estate properties in New York and Florida worth an estimated combined $75 million,[6] and none of which were reported to be purchased using digital assets.[7] This past week, on November 8, 2023, the U.K. added twenty-nine additional Russian individuals and entities operating in and supporting Russia's gold, oil, and other strategic sectors.[8] Simultaneously, the U.K. also issued a red alert to raise awareness of common evasion techniques used by enablers in the gold industry.[9]

Similarly, DOJ launched the National Cryptocurrency Enforcement Team (NCET)[10] to specifically target criminal actors using cryptocurrency or related technologies to move and transfer illicit funds. What I found as a prosecutor—and my experience is not unique—is that when criminals turn to digital methods, they actually leave breadcrumbs for investigators to follow. Baked into this technology are lines of code which make up the blockchain itself. When analyzed by sophisticated professionals, blockchain analytics help investigators follow the money in a way that they cannot with more traditional payment systems, such as outgoing international wire transfers from U.S. banks or cash transfers.

Importantly, there are already robust enforcement mechanisms enshrined in U.S. law to deal with the issues we are discussing today. The bigger question is whether U.S. authorities and law enforcement are adequately empowered and funded to enforce those laws that are already on the books. For instance, just because the means of exchange is crypto-based does not reduce a U.S. person's legal obligation to comply with U.S. economic sanctions, which would be the same as transferring fiat currency through a U.S. bank. So if a U.S.-based crypto exchange facilitates cryptocurrency transfers to Hamas, or a sanctioned country, they are violating U.S. law, and can be fined or prosecuted accordingly. As we are currently seeing, the issue is not necessarily U.S.-based crypto exchanges or U.S. based entities. Given the global nature of the blockchain many of the most challenging questions for lawmakers is how to ensure foreign entities are compliant.

(April 13, 2022), https://www.cnn.com/interactive/business/russian-oligarchs-yachts-real-estate-seizures/index.html.

6 Lucas, *supra* note 4.

7 Dareh Gregorian, *Here Are the Super Yachts Seized from Russian Oligarchs*, NBC News (May 22, 2022), https://www.nbcnews.com/politics/politics-news/are-superyachts-seized-russian-oligarchs-rcna20346.

8 Press Release, Foreign, Commonwealth & Development Office, National Crime Agency, and The Rt Hon James Cleverly MP, UK Cracks Down on Gold and Oil Networks Propping up Russia's War Economy (November 8, 2023), https://www.gov.uk/government/news/uk-cracks-down-on-gold-and-oil-networks-propping-up-russias-war-economy.

9 *Id.*; *See also*, the use of oil by Iran to attempt to circumvent sanctions. Press Release, U.S. Attorney's Office, District of Columbia, Largest U.S. Seizure of Iranian Fuel from Four Tankers (Aug. 14, 2020) https://www.justice.gov/usao-dc/pr/largest-us-seizure-iranian-fuel-four-tankers.

10 Press Release, U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

In April 2022, Secretary Yellen said, "we are aware of the possibility clearly that crypto could be used as a tool to evade sanctions, and we are carefully monitoring to make sure that doesn't occur. But I would say we have a good deal of authority in this area and are using it and will use it, and it is harder on a large scale for an economy to actually use crypto to evade sanctions. Even large-scale transactions would become apparent by those who regularly examine the blockchain. We would see that there were large transactions taking place. Exchanges, and those who use crypto need to get in and out of it to buy things in hard currencies and exchanges are subject to AML/CFT regulations. So, they are part of the financial system that is subject to those regulations."[11] Indeed, the traditional financial system remains a big avenue for illicit actors to evade sanctions and launder money. There is no means of exchange that is more anonymous than cash, which truly leaves no footprint, and there is no blockchain for cash.

Over the last month, in the wake of the heinous and barbaric terrorist attack on Israel, there were public reports about the use of digital assets by terrorist organizations. The analysis shows that terrorist organizations use diverse and sophisticated methods to facilitate their illicit activity, including through the use of global investment portfolios, *hawalas*, international exchanges, transfer of cash and remittances.[12] Of the methods described, only the movement of digital assets on a public blockchain can be traced in real time by anyone with access to the Internet. Moreover, administering fund flows in global investment portfolios requires the "gatekeepers" and third party facilitators that I used to investigate during my tenure at the DOJ.

It is clear that U.S. anti-money laundering and counter terrorist financing regulations must not be focused only on the use of digital assets but all aspects of the financial system, and the government must find ways to develop tools to address the rising illicit finance of foreign nations and autocratic regimes that could have devastating consequences for the U.S. democratic ideals and national security interests. We must also find safeguards without jeopardizing the rule of law and liberties such as privacy and financial inclusion.

Recommendations:

- Ensure that compliant U.S. based companies and projects in the digital asset ecosystem remain in the United States to avoid increased criminal activity offshore, a brain drain,

---

[11] The Annual Testimony of the Secretary of the Treasury on the State of the International Financial System: Hearing Before the Comm. on Financial Services, 117 Cong. 37 (April 6, 2022), https://www.govinfo.gov/content/pkg/CHRG-117hhrg47477/pdf/CHRG-117hhrg47477.pdf.

[12] Sam Lyman, *How Misinformation On Hamas And Crypto Fooled Nearly 20% Of Congress*, Forbes Digital Assets (Nov. 8, 2023), https://www.forbes.com/sites/digital-assets/2023/11/08/how-misinformation-on-hamas-and-crypto-fooled-nearly-20-of-congress/?sh=e3e3ef582706; Elliptic Team, *Setting the record straight on crypto crowdfunding by Hamas*, Elliptic Blog (Oct. 25, 2023), https://www.elliptic.co/blog/setting-the-record-straight-on-crypto-crowdfunding-by-hamas; Chainalysis Team, *Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing*, Chainalysis Blog, https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/.

technological decline, and further undermining of U.S. democratic ideals and national security interests.

    - Use whole of government tools to isolate autocratic and oppressive regimes that use technology to surveil their civilian communities, undermine basic liberties, and fund terrorists domestically and abroad.

- Lean into innovation through genuine sandboxes where the private sector could showcase in a prudent and compliant manner risk management tools that could be effective to protect and empower users. This will help ensure that before passing additional regulation we fully understand the technology and its uses.

    - Help further develop additional software to better leverage activity-based risk management on public ledgers, which is harder to spoof than static identities, as we see in the traditional finance world.

- Increase funding for government agencies like FinCEN, OFAC, DOJ and law enforcement for capacity building, increasing knowledge, expertise, and technology to more quickly and efficiently analyze large data sets (including suspicious activity reports) provided by financial institutions, centralized exchanges and other regulated and compliant actors in the digital asset space. This will help law enforcement proactively identify criminal networks, including sophisticated third party facilitators.

- Improve processes that already exist—adding precision and granularity in the information provided by regulated entities in suspicious activity reports (SARs), real time reporting, cross collaboration and information sharing between blockchain analytic firms.

- Develop and use blockchain technology to help the U.S. government and U.S. corporations from inadvertently funding illicit actors, terrorist organizations, or authoritarian governments. Using blockchain can help to prevent corruption in government procurement, counterfeit parts in law enforcement and military defense, and supply chains free of forced labor or sanctioned goods/funds (including from China[13], Russia), among other benefits.

- Promote education and engagement for both the public and private sector to ensure that new technology can be used by all sectors of society to help secure privacy, promote financial inclusion, and preserve national security interests.

- Lead cross-border collaboration between regulators and law enforcement to close gaps or prevent jurisdictions with poor or no regulatory frameworks to take advantage of U.S. or the international financial systems.

[13] Uyghur Forced Labor Prevention Act (UFLPA) (Public Law No. 117-78).

I. Blockchain Technology Can and Does Help Combat Illicit Finance

The U.S. government should use all tools available to combat illicit finance and counter terrorism in a thoughtful and prudent manner. I believe that digital technology can and does help combat illicit finance, but as with any instrument or method, it can be coupled with already existing systems to leverage its full potential and mitigate risk.

Virtual currency is a digital representation of value that functions as a medium of exchange. The exchange value of a particular virtual currency may be dependent on agreements between parties, and virtual currency can be both convertible (equivalent to the value of real currency) or non-convertible. Cryptocurrency is a form of virtual asset that uses cryptography to secure financial transactions.

Blockchain is a distributed ledger technology (DLT) that allows users to record messages in real time on a database that is public, transparent, and where the messages cannot be reversed. The base layer of a blockchain is distinct in that it operates through distributed nodes (computers that speak to each other), with no one centralized actor and no one single point of failure. Consensus mechanisms, as defined in the code of a blockchain, facilitate work by dictating how consensus gets done and by whom, and how these parties will be compensated to influence participant behavior. The unique nature of the blockchain has even been accepted by some state legislators as self-authenticating for evidentiary purposes.[14]

No Central Point of Control/Owner

The two most prevalent consensus mechanisms are proof-of-work (PoW) and proof-of-stake (PoS). Bitcoin and Ethereum were both PoW protocols until Ethereum's long-awaited transition to PoS occurred on September 15, 2022.[15] In PoW systems, participants, known as miners, expend effort to solve arbitrary mathematical hash computations to confirm transactions, create new blocks, and mine new digital assets. Miners compete with one another for valuable block rewards, either newly minted digital assets or payments in the native digital asset, and the computations needed to be performed create a level of difficulty that prevents gaming the system. Miners also function to secure the network because to attack a network would require 51% of the network's computing power, which would be an almost impossible endeavor.

PoS was introduced, in part, as an eco-friendly solution to the high energy consumption problem, and to provide a solution to inefficiencies of digital assets operating in a PoW consensus mechanism that inhibits scalability. Instead of miners, validators act as the server running the blockchain's network. Validators verify incoming additions to the blockchain's

---

[14] For example, Vermont enacted legislation declaring blockchain evidence self-authenticating. *See* 12 V.S.A. § 1913(b)(1) ("A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902.").

[15] Sam Kessler, *The Ethereum Merge Is Done, Opening a New Era for the Second-Biggest Blockchain*, CoinDesk (September 15, 2022), https://www.coindesk.com/tech/2022/09/15/the-ethereum-merge-is-done-did-it-work.

database and access to a record of historical activity and secure the network. PoS consensus mechanisms provide more transparency, equitability, a lower barrier of entry, and provide a higher throughput enabling scalability—thus increasing the potential participation—due to a greatly reduced need for specialized mining equipment, high energy costs and overall efficiency. As such, PoS systems include incentivization for long-term participation and building inherent trust by introducing a degree of transparency and punishing bad actors. Regardless of whether a blockchain operates as a PoW or PoS, because it does not have a central owner or operator, anyone can build applications or services on top of it.

Immutability

Immutability in the context of blockchain technology means the blockchain's ledger is permanent and unalterable. The ability for digital assets to be verified on a blockchain and available for anyone to see on the Internet makes it easier for law enforcement to follow the movement of those assets in real time. Blockchain's immutability also allows law enforcement to view all transaction history, for all time, associated with any wallet address involved in a known transaction.[16] When a prosecutor or law enforcement has information about the source of potential "dirty" funds, a grand jury subpoena or other court authorized process can be used to obtain information from a centralized exchange or custodial service provider. The immutability of the blockchain coupled with its traceability is critical to investigations being effective. Immutability is also critical to preserving evidence to be admissible in court. Moreover, no matter how long an investigation or trial will take, the blockchain data will be there and will remain the same.[17] This information could also be used to corroborate witness testimony, and help to seize, restrain, and forfeit proceeds or assets involved in the criminal activity. In victim crimes, this information is critical to helping victims obtain restitution and forfeiture.

---

[16] Alexandra D. Comolli and Michele R. Korver, *Surfing the First Wave of Cryptocurrency Money Laundering*, 69 DOJ J. FED. L. & PRAC., no. 3, 2021 at 185 ("As such, even if an individual uses a different address for every transaction, the historical trail from the present, Z, to the past, A, will be transactionally connected. This means that, if law enforcement can tie wallet address Z to Jane Doe, all transactions from Z to A may also have a connection to her. Thus, blockchains may, in some respects, be worse for criminals than cash because any operational security failure may allow all their transactions to be linked to them—whereas cash has no ledger associated with it.").

[17] Sanjeev Bhasker, Alexandra D. Comolli, and Olivia Zhu, *Carpe Crypto: Prosecuting Cases Involving Digital Assets and Blockchain Technology*, 70 DOJ J. FED. L. & PRAC., no. 4, 2022, at 110 ("The public blockchain enables investigators to trace funds forwards and backwards from a single address or a single transaction, akin to how investigators trace the movement of funds in fiat currencies. Yet, unlike more traditional bank records, the blockchain does not identify the sender or receiver, apart from the public addresses. It is here that blockchain analysis brings the great irony of digital assets front and center: The need to cash out (that is, convert) digital assets into traditional currency remains the reality. Some virtual asset service providers (VASPs), such as cryptocurrency exchanges, provide the all-important on and off ramps connecting the "real world" and the "virtual world." VASPs, which are generally recognized as money service businesses (MSBs) domestically, are regulated in the United States under the Bank Secrecy Act and respond to legal process with valuable attribution evidence—a result of their anti-money laundering recordkeeping obligations (thank you, FinCEN!).").

Pseudonymity

During my tenure at the DOJ, one of the biggest misnomers about digital assets and the blockchain was that digital assets were anonymous.[18] Digital assets such as "bitcoin" operate on ledgers with the use of addresses, or a long string of alphanumeric characters. Although the ledgers do not contain what we ordinarily see as a first and last name of an individual, the information on the blockchain can be used to identify individuals by analyzing the transactions between an individual's address and third parties. For example, transactions on the ledger that connect to a centralized exchange or custodial service provider would allow law enforcement to seek information that U.S. regulated exchanges are required to collect as part of their anti-money laundering and know your customer (KYC) requirements.

There are methods, however, that allow individuals to maintain privacy or obscure information or connections between wallet addresses. One example is Anonymity Enhanced Cryptocurrencies (AECs), sometimes referred to as "privacy coins",[19] which may use obscured blockchains to limit traceability of the assets. The liquidity for AECs is fairly low, and much less than Bitcoin or other digital assets,[20] so it is less likely that AECs will be used for purposes of illicit activity instead of alternative financial instruments. As Treasury Secretary Yellen testified in April 2022, using crypto to engage in illicit activity on a large scale "is not easy to do…"[21] and would likely require an individual to exchange AECs for more liquid digital assets, such as Bitcoin or another digital asset that would be visible on a public blockchain. In addition, in September 2023, after what appears to have been a hack of a Monero wallet, despite Monero's complexity of transaction graphs, blockchain tracing helped identify the potential hacker using heuristic evidence.[22] As such, while the risk of these assets being used to launder funds or to engage in illicit activity may be less than compared to other methods of money laundering simply because they are less available to bad actors, there are also now more tools available to mitigate the risks that do exist.

---

18 Matthew J. Cronin, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*, 66 U.S. ATT'YS BULL., no. 4, 2018, at 71 ("Criminals believe that cryptocurrency is anonymous. That is only partially correct. While no one needs to reveal their identity to open a Bitcoin wallet and transact in bitcoins, all transactions are recorded and available to the public on the blockchain. Reviewing criminally related transactions on the blockchain offers similar insight into a criminal organization as a review of financial services data.").

19 *See, e.g.,* Monero, *https://www.getmonero.org/* Dash, https://www.dash.org/; and Zcash, https://z.cash/.

20 *See generally* https://coinmarketcap.com/; https://www.coingecko.com/.

21 Annual Testimony of the Secretary of the Treasury, *supra* note 11.

22 Jamie Redman, *Moonstone Research Study Etches Doubts on Monero's Privacy; Crypto Community Reacts*, Bitcoin.com (November 5, 2023), https://news.bitcoin.com/moonstone-research-study-etches-doubts-on-moneros-privacy-crypto-community-reacts/.

Speed of Transactions

Digital asset transactions have near-instant settlement. While instant settlement could make it more difficult for law enforcement to stop the movement of funds, the traceability of digital assets on the blockchain, even through peer to peer transactions, is more transparent than if criminals use cash or prepaid cards (or gift cards).[23] Victims who are elderly, vulnerable, or fall prey to a business compromise or romance scam could have their bank accounts drained instantaneously. If those funds are converted into cash, it could be almost impossible for law enforcement to identify the perpetrators. When I was prosecutor at the New York County District Attorney's Office, I investigated cases where defendants forced employees or contractors to cash checks through regulated check cashers only to confiscate the cash from the victims. The cash would be nearly impossible to trace, including how to prove that the cash was later deposited in a defendant's accounts.

Applications of Blockchain Technology in Traditional Finance

In addition to the permissionless blockchains, there are now growing numbers of permissioned applications for blockchain technology. Traditional financial institutions are also incorporating blockchain technology into their systems. Last Friday, JPMorgan announced that it had launched programmable payments or automatic execution of payments on its permissioned blockchain-based payments system, JPM Coin.[24] Citi announced a pilot, Citi Token Services, for cash management and trade finance, where the bank uses blockchain and smart contract technologies to deliver digital asset solutions for institutional clients. Citi stated that it believes its institutional clients have an "always-on" need for programmable financial services.[25] The ability of these traditional financial institutions to adopt new uses for this technology can further enable combating illicit activity with the current BSA framework.

II. AML/CFT Requirements Preventing Illicit Finance in the Digital Asset Ecosystem

The U.S. has robust anti-money laundering and counter terrorist financing laws and regulations. As the financial sector and economy become more global and interconnected, the ways in which sophisticated criminal networks attempt to exploit the financial sector evolves. In the last two years we have seen autocratic regimes and terrorist organizations exploit the

---

[23] FinCEN, Ruling 2003-4, *Definition of Money Transmitter/Stored Value (Gift Certificates/Gift Cards)* (Aug. 15, 2003), https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/definition-money-transmitterstored-value-gift; Gregory T. Parks, et. al., *New Gift Card Rules from FinCEN*, National Law Review (Dec. 26, 2021), https://www.natlawreview.com/article/new-gift-card-rules-fincen.

[24] Yogita Khatri, *JPM Rolls Out Programmable Payments via JPM Coin*, The Block (November 10, 2023), https://www.theblock.co/post/262595/jpmorgan-jpm-coin-programmable-payments.

[25] Press Release, Citi Group, Citi Develops New Digital Asset Capabilities for Institutional Clients (September 18, 2023), https://www.citigroup.com/global/news/press-release/2023/citi-develops-new-digital-asset-capabilities-for-institutional-clients.

international and the U.S. financial systems to facilitate and fund their criminal activities. These issues are not limited to the digital assets space.

General Overview of the Bank Secrecy Act of 1970

The backbone of the United States' efforts to combat money laundering and financial crime comes from the Bank Secrecy Act of 1970 (BSA).[26] It was designed to help prevent criminals from exploiting the U.S. financial institutions, especially from the use of cash.[27] Under the BSA, financial institutions, including banks, money service businesses (MSBs), payment processors, casinos and others are required to report: (1) currency transactions by any person of more than $10,000 in cash each day; and (2) suspicious activity when they believe that a financial transaction or series of transactions (a) involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity; (b) is designed to evade regulations promulgated under the BSA; or (c) lacks a business or apparent lawful purpose. The BSA and its implementing regulations require domestic banks and other financial institutions to establish and maintain programs to detect and report suspicious activity, and to maintain certain records where "they are highly useful . . . in criminal, tax, or regulatory investigations and proceedings."[28]

Financial institutions must make certain disclosures, including filing Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), and other reports pursuant to their BSA obligations. In addition, financial institutions are required to maintain programs of compliance against money laundering.[29] Pursuant to 31 U.S.C. § 5318(h)(1) and 12 C.F.R. § 21.21, a financial institution must establish and maintain (and have a culture of compliance) an anti-money laundering compliance program that at a minimum:

i. Provides internal policies, procedures, and controls designed to guard against money laundering;
ii. Provided for a compliance officer to coordinate and monitor day-to-day compliance with the BSA and AML requirements;
iii. Provide for an on-going employee training program; and
iv. Provided for independent testing for compliance conducted by bank personnel or an outside party.

---

[26] 31 U.S.C. § 5311, *et seq*.

[27] *See, e.g.*, 31 CFR § 1022.210(a) (requiring money services businesses to have "[a]n effective anti-money laundering program … that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities."); Steven M. D'Antuono, *Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform*, Statement Before the Senate Banking, Housing, and Urban Affairs Committee, Washington, D.C. (Nov. 29, 2018) ("Cash transactions are particularly vulnerable to money laundering. Cash is anonymous, fungible, and portable; . . . it is used and held around the world; and is difficult to trace once spent.").

[28] 31 U.S.C. § 5311(1)(A).

[29] 31 U.S.C. § 5318(a)(2).

In 2013, FinCEN issued guidance applying the basic principles of the BSA to the digital asset and cryptocurrency industry.[30] FinCEN's guidance imposed the same BSA and record-keeping requirements on intermediaries who act on behalf of customers in the digital asset ecosystem as required of MSBs. Further, in 2019, FinCEN issued additional guidance that identified "unhosted wallets" as software that allowed individuals independence over their own digital assets, meaning individuals could hold digital assets themselves without a third-party intermediary.[31] (This is in contrast to a custodial service provider that maintains custody of a third party's digital assets.) Moreover, the FinCEN 2019 guidance provided additional guidance to help identify suspicious cryptocurrency transactions and the type of information that should be included in SARs.[32] The BSA and the FinCEN guidance calls for regulated entities to engage in a risk-based approach, similar to financial institutions that must evaluate their risk and establish guardrails that are appropriate for those risks. The BSA does not require that a large, national bank have the same AML and CFT policies as a smaller community bank.

In 2021, Congress also passed the Anti-Money Laundering Act (AML Act),[33] which included several provisions related to beneficial ownership, expanded U.S. law enforcement authority to obtain records from *foreign* financial institutions with correspondent accounts in the U.S. through a grand jury and trial subpoena,[34] and further codified FinCEN's previous position that the definition of a financial institution and money transmission business included businesses involved in the transmission or exchange of "value that substitutes for currency."[35]

The regulatory framework set forth by the BSA and further expanded by AML Act as it directly relates to digital assets is also supported by international bodies, including, the Financial

---

30 FinCEN, FIN–2013–G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,* Mar. 18, 2013, https://www.fincen.gov/sites/default/files/guidance/FIN-2013-G001.pdf.

31 FinCEN, FIN–2019–G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,* May 9, 2019, *https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.*

32 FinCEN, FIN-2019-A003, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (May 9, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

33 *See* Pub. L. No. 116–283, §§ 6001-6511, 134 Stat. 3388 (2021).

See Pub. L. No. 107-56, § 302(b)(4), 115 Stat. 272, 297 (2021).

34 Pub. L. No. 116–283, §§ 6001-6511, 134 Stat. 3388 (2021).

35 FinCEN, FIN–2013–G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,* Mar. 18, 2013, https://www.fincen.gov/sites/default/files/guidance/FIN-2013-G001.pdf; *see also* FIN–2019–G001, *supra* note 32.

Action Task Force (FATF). In 2018 and again in 2021,[36] FATF made clear that Virtual Asset Service Providers (VASPs) were subject to the same obligations as traditional financial institutions, including requiring VASPs to implement AML/CFT programs that include:

- risk assessments,
- customer due diligence,
- record keeping,
- filing suspicious activity reports,
- conducting sanctions screening, and
- complying with Recommendation 16 "Travel Rule"[37]

A March 2022 survey conducted by the FATF found that only 29 of 98 jurisdictions at that time passed the requirements to comply with the Travel Rule, and only a small subset of the jurisdictions started enforcement.[38] This past July 2023, FATF once again urged countries to implement the requirements for VASPs to close the loopholes that could be exploited for illicit finance.[39]

Blockchain-Based Compliance Technologies Can Provide More Effective Safeguards to Combating Illicit Finance

The United States centralized exchanges and fiat on-off ramps[40] are considered MSBs that must comply with BSA obligations.

As discussed above, blockchains preserve all transactions and record them on a public ledger. This means that centralized exchanges or VASPs (as referred to by FATF) can identify and analyze transactions on the blockchain, regardless of whether the specific transaction

---

[36] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021), www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html.

[37] Financial Action Task Force, *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (June 27, 2023), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html. Specifically with respect to the Travel Rule, VASPs were to obtain, hold and transmit required information about the originator and beneficiary of funds. *Id.*

[38] Financial Action Task Force, *Targeted Update on Implementation of FATF's Standards on VAs and VASPs* (June 30, 2022), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html#:~:text=Of%20the%2098%20jurisdictions%20that,these%20jurisdictions%20have%20started%20enforcement.

[39] Financial Action Task Force, *Outcomes FATF Plenary, 21-23 June 2023* (June 23, 2023), https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2023.html.

[40] An "on-ramp" is a service that would allow the transfer or exchange of fiat currencies, such as the U.S. dollar for a digital asset (Bitcoin, Ether, etc.), whereas an "off-ramp" allows the transfer or exchange of a digital asset for fiat. These services are already regulated in the United States under the BSA as described above.

occurred on their platform.[41] This is in contrast to a traditional financial institution, which may only have visibility into the customers or transactions that occur within that specific banking institution. Moreover, blockchain analytics firms can help centralized exchanges and others in the digital asset ecosystem to ensure compliance with BSA requirements, and help identify suspicious activity that centralized exchanges can report in SAR filings, and as needed, cooperate with law enforcement.[42] The information collected by law enforcement could be critical to conducting investigations, identifying assets, co-conspirators or victims, and seizing or freezing assets.

Centralized exchanges and custodial service providers can also implement "know your transaction" (KYT) monitoring to ensure they meet their AML/CFT needs.[43] While KYC processes help institutions and centralized exchanges assess potential risk through identity verification, KYT analyzes the data from every financial transaction. As such, sanctions compliance and AML/CFT is expanded to include transactional data that is not limited only by direct transactions between parties but also includes multiple hops and counterparties providing a much more robust assessment of counterparty risk and potential sanctions exposure. Coupling KYC and KYT, a compliant VASP or fiat on-off ramp would be more able to take reasonable measures against money laundering, terrorist financing and fraud.

For example, as customers onboard with an exchange or a custodial wallet provider, the regulated entity will have the customer's wallet address and IP address in addition to other standard due diligence information. If necessary, this information can be shared with law enforcement, and law enforcement would be able to trace the digital asset transactions in real time and request that an exchange freezes illicit funds held in the wallet(s).

Using the information collected through KYC/KYT, compliant entities can share more developed data with law enforcement when filing already required SARs, which improves law enforcement's ability to identify and investigate criminal networks.[44] The data provided to law enforcement from the blockchain will not change even if located abroad and obtained through

---

41 *See* Ari Redbord, et al., *Home Alone? Never, with Transaction Monitoring,* (Sept. 22, 2022), https://www.acamstoday.org/home-alone-never-with-transaction-monitoring/ (emphasizing how "the blockchain allows for unprecedented visibility on financial flows.").

42 *See* Anastasios Balaskas and Virginia N.L. Franqueira, *Analytical Tools for Blockchain: Review, Taxonomy andOpen Challenges*, Int'l Conf. on Cyber Security and Protection of Digital Services, at 5 (2018), https://core.ac.uk/download/pdf/200747549.pdf ("Blockchain analytic tools can offer law enforcement agencies considerable benefits" as they "could have all the needed records in order to trace transferred money, something that would not necessarily be feasible within the traditional economy."); Michele R. Korver, et al., *Attribution in Cryptocurrency Cases*, 67(1) Department of Justice Journal of Federal Law and Practice 246 (Feb. 2019) ("Armed only with the knowledge of a target's cryptocurrency address and this single—but highly valuable—data set, law enforcement can learn a myriad of vital pieces of information about a target.").

43 *See, e.g.,* https://withpersona.com/blog/know-your-transaction-kyt.

44 FIN–2019–G001, *supra* note 32.

the Mutual Legal Assistance Treaty (MLAT) process, which is too slow even for traditional and contemporary cross border investigations.[45]

Even if a criminal uses a self-hosted (or unhosted) wallet, when the criminal needs to exchange the digital asset to fiat, the individual will still be required to use an "off-ramp" in order to convert to fiat currency. Once the funds move to a centralized exchange or custodial service provider, AML/KYC screening will be conducted under the BSA requirements. Using blockchain technology to assess a particular customer's transactions or wallet activity allows dynamic assessments of a customer or wallet's risk – which could be deemed low risk at the time of on-boarding but then be high risk later. In this situation, the centralized exchange or custodial service provider could request additional due diligence, enhance monitoring if wallet activity includes interactions with higher risk jurisdictions, engage in IP address monitoring, file a SAR or freeze the wallet's funds.[46]

The ability of participants to see across blockchain platforms contrasts with the available information from traditional financial institutions. A bank may only have information related to a client's activity or due diligence relative to that client's activities at that bank. Even the level of due diligence banks apply to retail or private bank clients may differ and would require coordination within the bank to identify any information that may be suspicious. When conducting an investigation, law enforcement must also be careful to ensure that the bank does not close an account after receiving a grand jury subpoena, otherwise valuable information could be lost since it is not maintained on an immutable ledger.

Additionally, a traditional financial institution could be filing a SAR on one transaction or multiple transactions but no other financial institution may know of the existence of a SAR or that the customer of the bank is accused of engaging in illicit activity. In contrast, all transactions on public blockchains are visible to anyone using the Internet, which means that information that may be identified and flagged by a VASP would be available to other actors across blockchains. Importantly, compliant VASPs that are encouraged to transact with self-hosted wallets would also be able to report on any suspicious activity or transactions that occurred from that wallet. The information tracked, maintained, and if necessary documented in a SAR or shared with law enforcement would be helpful for mitigating the risk of money laundering or terrorist financing associated with self hosted wallets.

Compliance by U.S. Digital Asset Ecosystem Participants

The above described BSA requirements are already being implemented by ecosystem participants to trace illicit flows of digital assets, filing SARs, cooperating with law enforcement, and when necessary, freezing assets. For example, in 2020, at the request of law enforcement,

---

45 Evan Norris and Morgan J. Cohen, *How US Authorities Obtain Foreign Evidence in Cross-Border Investigations,* Global Investigations Review (Oct. 13, 2020), https://globalinvestigationsreview.com/review/the-investigations-review-of-the-americas/2021/article/how-us-authorities-obtain-foreign-evidence-in-cross-border-investigations.

46 Chainalysis Team, *How Chainalysis Helps Compliance Teams Address Sanctions Red Flags* (March 8, 2022), https://blog.chainalysis.com/reports/fincen-russia-sanctions-red-flags-chainalysis/.

over 100,000 USDC was frozen and a certain address was blacklisted, demonstrating that even when there is activity between a decentralized application and a U.S. regulated business, affirmative compliance and sanctions compliance occurs.[47] Similarly, when a hack occurred earlier this year, swift action was taken to freeze funds by the U.S.-based entity.[48] In addition, on August 8, 2022, when OFAC sanctioned Tornado Cash,[49] U.S.-based stablecoin issuers had the ability to immediately blacklist interactions with the Tornado Cash application on the Ethereum smart contract level and could freeze funds in wallets designated by OFAC.[50] Additionally, just a few days ago, another U.S.-based entity made changes to ensure compliance with the FATF's Travel Rule.[51] The ability to freeze wallet addresses on the secondary market in compliance with U.S. sanctions is unique to blockchain technology.

III. Utilizing Digital Assets for Illicit Activity

The United States has been on the forefront of innovation, and it is this innovation that drives society forward. With innovation comes the need to balance the benefits with the potential of bad actors to misuse the technology, but that does not mean that the technology or tools should be dismissed or banned.

---

47 Nikhilesh De, *Circle Confirms Freezing $100K in USDC at Law Enforcement's Request*, CoinDesk (July 8, 2020), https://www.coindesk.com/markets/2020/07/08/circle-confirms-freezing-100k-in-usdc-at-law-enforcements-request.

48 Lacton Muriuki, *Circle Freezes $63M in USDC after Multichain Hack*, Cryptopolitan (July 7, 2023), https://www.cryptopolitan.com/circle-freezes-63m-in-usdc-multichain-hack.

49 Press Release, U.S. Department of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (August 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

50 Zhiyuan Sun, *Circle Freezes Blacklisted Tornado Cash Smart Contract Addresses*, Cointelegraph (August 8, 2022), https://cointelegraph.com/news/circle-freezes-blacklisted-tornado-cash-smart-contract-addresses; *Cf.* Ornella Hernandez, *Tether Won't Freeze Sanctioned Tornado Cash Addresses Without Authorities' Request*, Blockworks (August 24, 2022), https://blockworks.co/news/tether-wont-freeze-sanctioned-tornado-cash-addresses-without-authorities-request.

51 Brayden Lindrea, *Gemini's Travel Rule Measures Reflect 'Worrying Creep' of Overregulation*, Cointelegraph (Nov. 9, 2023), https://cointelegraph.com/news/gemini-travel-rule-trust-crypto-transfer-restrictions-hurt-self-custody-trezor.

As has been the case in traditional financial institutions,[52] art and antiquities,[53] real estate, and real property,[54] sophisticated actors use different means and methods to engage in money laundering and illicit finance. Similarly, there are bad actors who use digital assets to commit crimes. Chainalysis reported that in 2022, the percentage of all cryptocurrency activity associated with illicit activity was 0.24%, which rose from 0.12% in 2021, and was the first time that this figure rose since 2019. It is important to understand the nature, methods, means and jurisdictions through which the illicit activity occurred to best tailor an appropriate response.

Fraud

Criminals and criminal networks commit fraud. In my experience as a prosecutor, I investigated mortgage fraud,[55] exploitation of national school lunch programs,[56] fraudulent employment and immigration documents,[57] and different types of scams.[58] At the heart of many fraud schemes is social engineering, including exploitation of a personal relationship or vulnerability. In many of these cases, traditional financial institutions are used to wire funds,

---

52 Bob Van Voris, *Deutsche Bank, Standard Chartered Sued Over Afghanistan Dead*, Bloomberg (Aug. 5, 2021), https://www.bloomberg.com/news/articles/2021-08-05/deutsche-bank-standard-chartered-sued-over-afghanistan-deaths#xj4y7vzkg (DB and Standard charter sued for providing aid to terrorist organization); Pete Schroeder and Chris Prentice, *US Fed Fines Deutsche Bank $186 Million for Slow Progress against Money Laundering*, Reuters (July 19, 2023), https://www.reuters.com/business/finance/fed-fines-deutsche-bank-186-mln-insufficient-progress-addressing-anti-money-2023-07-19/.

53 Financial Action Task Force, *Money Laundering and Terrorist Financing in the Art and Antiquities Market* (Feb. 27, 2023), https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html.

54 Press Release, U.S. Department of Justice, $300 Million Yacht of Sanctioned Russian Oligarch Suleiman Kerimov Seized by Fiji at Request of United States (May 5, 2022), https://www.justice.gov/opa/pr/300-million-yacht-sanctioned-russian-oligarch-suleiman-kerimov-seized-fiji-request-united.

55 *E.g.,* Press Release, U.S. Attorney's Office, Southern District of California, *Former San Diego Police Officer and Three Others Sentenced for Crimes Stemming from Years-long Operation of Illicit Massage Businesses* (Oct. 13, 2023), https://www.justice.gov/usao-sdca/pr/former-san-diego-police-officer-and-three-others-sentenced-crimes-stemming-years-long.

56 *E.g.,* Tom Hayden, *Tearful Former School District Employee Denies Seeking Free Lunches for Daughter*, NJ.com (Mar. 9, 2016), https://www.nj.com/union/2016/03/tearful_former_school_employee_denies_seeking_free.html.

57 *E.g.,* Press Release, U.S. Attorney's Office, Southern District of Georgia, *Human Smuggling, Forced Labor among Allegations in South Georgia Federal Indictment* (Nov. 22, 2021), https://www.justice.gov/usao-sdga/pr/human-smuggling-forced-labor-among-allegations-south-georgia-federal-indictment.

58 *See, e.g.,* Press Release, U.S. Attorney's Office, Southern District of Texas, Out of state group charged in $11M Indian call center fraud ring (Oct. 11, 2022), https://www.justice.gov/usao-sdtx/pr/out-state-group-charged-11m-indian-call-center-fraud-ring.

open business or personal accounts through which illicit funds flow, facilitate the use of cash, and now more recently, transact in digital assets.

Over the last few years there have been increased reports of "pig butchering."[59] These scams are similar to other social engineering exploits and may involve a perpetrator identifying and grooming a victim through the use of a personal relationship to cause the victim to invest in fake projects or steal funds. Victims could be contacted through dating applications, social media, or text messages, and then after developing a relationship, the victim may end up investing in what is ultimately a fraudulent company or scheme. In some cases involving virtual asset wallet applications, victims' vulnerabilities are exploited and the victim provide full access and control of their wallets to the scammers. The ability to trace these transactions on the blockchain in addition to the evidence that could be collected from social media accounts and other sources could prove helpful to law enforcement.

Mixers

In certain cases, individuals could use "mixers" or a type of software service that allows digital assets to be mixed together with other individual's funds before being sent to the ultimate recipient. As FinCEN noted in its recent NPRM, there are both licit and illicit purposes of using a mixing service; FinCEN also notes that the national security risks arising from illicit money laundering lies outside the United States.[60] In other words, it is the lack of accountability and strong AML/CFT policies abroad that could jeopardize the United States' financial security.

In my experience as a prosecutor, the use of "mixing" services in the digital asset space is similar to the use of funnel accounts in traditional finance.[61] Funnel accounts could be set up by multiple people across the country or in different countries; or multiple accounts could be opened by the same person. Funds would be deposited into these accounts and then sent to a third-party account and ultimately to the final recipient. In some instances, these funnel accounts would be set up to allow for multiple deposits under the $10,000 reporting requirement under the BSA. Funnel accounts also allow bad actors to quickly open and close accounts to evade law enforcement detection. Unlike when a potential criminal network opens multiple wallets or

---

[59] *See* U.S. Department of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* (April 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[60] FinCEN, FINCEN–2023–0016, *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, 88 FR 72701 (Oct. 23, 2023), https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions; Press Release, FinCEN, *FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing* (Oct. 19, 2023), https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency, ("[t]he lack of transparency surrounding international CVC mixing activity is an acute money laundering and national security risk, and increasing transparency in connection with this activity is a key component to denying illicit actors access to the U.S. and global financial systems.").

[61] FinCEN, FIN-2023-Alert001, *FinCEN Alert on Human Smuggling along the Southwest Border of the United States* (Jan. 13, 2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf.

transfers through mixers that can then be transferred to other wallets on the blockchain, there is no ledger for funnel account data. This makes it more difficult for law enforcement to quickly seize assets or freeze funds in funnel accounts.

Moreover, unlike cash, digital assets moving on a blockchain are easier for law enforcement to track, as the public ledger contains the date and time of transaction, specific virtual asset and amount transacted, wallet address, and additional unique transaction identification. Law enforcement can trace the entire transaction history (and conduct real-time on-chain surveillance) not only related to that specific transaction but the history of all transactions in the identified wallet address.

Hacks

Criminal networks from autocratic regimes like Russia, North Korea, and elsewhere have engaged in hacks and other cybercrime well before the more notable "crypto" related hacks. In 2013, the Department of Justice indicted five Russian hackers related to a sophisticated and at the time "cutting edge" "SQL (Structured Query Language) injection attack," which used a sophisticated programming language designed to manage data held in particular types of databases, identified vulnerabilities in SQL databases, and used those vulnerabilities to infiltrate a computer network.[62] Once they gained entry into the network they placed malicious code or malware on the system, created a back door that made the system vulnerable, and stole data including 160 million credit card numbers and over $300 million from large companies including Heartland.[63]

In 2018,[64] Treasury sanctioned the North Korean Lazarous group. At the time, Treasury stated that the group used phishing and backdoor intrusions to successfully target more than sixteen organizations across eleven countries, including the SWIFT messaging system, financial institutions, and cryptocurrency exchanges. One such example includes the theft of approximately $80 million from the Central Bank of Bangladesh's New York Federal Reserve account: "By leveraging malware similar to that seen in the SPE cyber attack, Bluenoroff and Lazarus Group made over 36 large fund transfer requests using stolen SWIFT credentials in an attempt to steal a total of $851 million before a typographical error alerted personnel to prevent

---

62 Press Release, U.S. Department of Justice, *Five Indicted in New Jersey for Largest Known Data Breach Conspiracy* (July 25, 2023), https://www.justice.gov/opa/pr/five-indicted-new-jersey-largest-known-data-breach-conspiracy; Press Release, U.S. Department of Justice, *Leader of Hacking Ring Sentenced for Massive Identity Thefts from Payment Processor and U.S. Retail Networks* (Mar. 26, 2010), https://www.justice.gov/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail.

63 Kelly Jackson Higgins, *Russian Hackers Sentenced in Heartland Payment Systems Breach Case, DarkReading* (Feb. 16, 2018), https://www.darkreading.com/attacks-breaches/russian-hackers-sentenced-in-heartland-payment-systems-breach-case.

64 Press Release, U.S. Department of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774.

the additional funds from being stolen."[65] Simultaneously with Treasury's sanctions designation, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Cyber Command (USCYBERCOM) worked together to disclose malware examples to the private cyber security sector to help proactively protect the U.S. financial system and critical infrastructure.[66]

The Lazarous group has continued to expand its illicit activity, including targeting the digital asset ecosystem. The methods, however, remain the same—exploiting computer programming vulnerabilities. The Ronan hack was committed by compromising computers known as nodes, operated by the Axie Infinity Maker Sky Mavis and the Axie DAO, that supported the bridge that enables converting digital assets to be used on another network.[67] The compromised private keys were used to forge fake withdrawals. Information from the blockchain, visible to anyone on the Internet, helped identify the wallet where the stolen funds were being held—an Ethereum address which was also tied to an offshore centralized exchange. Using blockchain forensics, Treasury was able to trace and identify that the Ethereum wallet belonged to the Lazarus group.[68] This is an example where the importance of cyber security and improvements to the technology are critical to combating the exploitation of the technology.[69]

In addition to using the blockchain to identify and designate bad actors under Treasury's sanctions authorities related to hacks in the digital asset space, the DOJ has successfully been able to identify, investigate, prosecute and convict money launderers after hacks of an exchange even years later. In February 2022, the U.S. Attorney's Office in the District of Columbia used money laundering and other criminal authorities to charge two defendants with stealing over $3.6 billion dollars from a 2006 hack of the Bitfinex network, which authorized over 2,000 transactions.[70] At the time of the indictment, U.S. Attorney Graves stated that "[t]he Department

---

65 *Id.*

66 *Id*.

67 *See* Andrew Thurman, *Axie Infinity's Ronin Network Suffers $625M Exploit*, CoinDesk (Mar. 29, 2022), https://www.coindesk.com/tech/2022/03/29/axie-infinitys-ronin-network-suffers-625m-exploit/; Olga Kharif, *Hackers Steal About $600 Million in One of the Biggest Crypto Heists*, Bloomberg (Mar. 29, 2022), https://www.bloomberg.com/news/articles/2022-03-29/hackers-steal-590-million-from-ronin-in-latest-bridge-attack#xj4y7vzkg.

68 Ryan Browne, *U.S. Officials Link North Korean Hackers to $615 Million Cryptocurrency Heist*, CNBC (April 15, 2022), https://www.cnbc.com/2022/04/15/ronin-hack-north-korea-linked-to-615-million-crypto-heist-us-says.html.

69 The Harmony bridge exploit was also reported to have been related to security loopholes in the bridge that was exploited by the Lazarus Group. Brian Quarmby, *North Korea's Lazarus Group Masterminded $100M Harmony Hack: FBI Confirms*, CoinTelegraph (Jan. 24, 2023), https://cointelegraph.com/news/north-korea-s-lazarus-group-masterminded-100m-harmony-hack-fbi-confirms.

70 Press Release, U.S. Attorney's Office, District of Columbia, *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency* (Feb. 8, 2022), https://www.justice.gov/usao-dc/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

of Justice and our office stand ready to confront these threats by using 21st century investigative techniques to recover the stolen funds and to hold the perpetrators accountable."[71] As detailed in the Statement of Facts filed with the Indictment, the transparency of the blockchain allowed law enforcement to trace all the steps taken in an attempt to conceal the hacked funds, which may not have been possible if a similar theft occurred without a public blockchain.[72]

Terrorist Financing

After the terrorist attack on the World Trade Center in 1993 and then again after September 11, 2001, reports and analysis showed that charities were being used to fund terrorism.[73] There were many reports that identified small amounts of money being transferred through traditional financial institutions to alleged charities, which turned out to be shell companies for terrorist organizations.[74] Unfortunately, terrorist organizations have solicited donations in the form of digital assets too.[75] However, accurate data about the alleged use of digital assets by Hamas and other terrorist organizations after the horrific terrorist attack on Israel on October 7, 2023, is harder to confirm.[76]

For example, in 2019, reports showed that Hamas was using Bitcoin to fund their activities.[77] Fast forward to April 2023, and it would appear that Hamas was urging its supporters not to send digital assets.[78] One article inaccurately described that "Bitcoin" and

---

71 *Id.*

72 *See United States v. Ilya Lichtenstein, 22-mj-00022-RMM, ECF No. 1-1 (Feb. 7, 2022), available at https://www.justice.gov/opa/press-release/file/1470211/download.*

73 National Commission on Terrorist Attacks Upon the United States, *Chapter 1: Introduction and Executive Summary*, Terrorist Financing Staff Monograph, https://9-11commission.gov/staff_statements/911_TerrFin_Ch1.pdf.

74 Matthew Levitt, Charitable Organizations and Terrorist Financing: A War on Terror Status-Check, The Washington Institute for Near East Policy (March 19, 2004), https://www.washingtoninstitute.org/policy-analysis/charitable-organizations-and-terrorist-financing-war-terror-status-check#:~:text=The%20International%20Islamic%20Relief%20Organizations,Islamic%20Relief%20Organizations%20(IIRO).

75 Tom Wilson and Dan Williams, *Hamas Shifts Tactics in Bitcoin Fundraising, Highlighting Crypto Risks: Research*, Reuters (April 26, 2019), https://www.reuters.com/article/ctech-us-crypto-currencies-hamas-idCAKCN1S20FA-OCATC.

76 Sam Lyman, *How Misinformation On Hamas And Crypto Fooled Nearly 20% Of Congress*, Forbes (Nov. 8, 2023), https://www.forbes.com/sites/digital-assets/2023/11/08/how-misinformation-on-hamas-and-crypto-fooled-nearly-20-of-congress.

77 Nidal Al-Mughrabi, *Hamas Armed Wing Announces Suspension of Bitcoin Fundraising*, Reuters (April 28, 2023), https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28.

78 *Id.*

other digital assets provided "high levels" of anonymity to Hamas,[79] which has been refuted by law enforcement and prosecutors. And a now-debunked report by the Wall Street Journal alleged that blockchain data showed that $130 million in cryptocurrency was raised to fund the war on Israel, which was subsequently corrected to say that "Palestinian Islamic Jihad and Hezbollah may have exchanged up to $12 million in crypto since 2021, according to crypto-research firm Elliptic . . . ."[80]

Notably, the Wall Street Journal also reported that researchers who study Hamas' financing methods have found that the use of crypto by Hamas remains only one of a number of methods used. The researchers noted the transport of cash from Egypt to Gaza, and Hamas funding from Tehran (Iran) of roughly $100 million a year."[81] If accurate, this means that more must be done by foreign jurisdictions to prevent cash and traditional financial instruments from being used to fund terrorism. It is also critical to find effective ways to ensure compliance by foreign centralized exchanges. This data also suggests that U.S. based centralized exchanges are either not being used by illicit actors or the already existing AML/CFT requirements to mitigate risk of sanctions evasion, illicit finance, and terrorist financing flowing through the U.S. financial system are working. But the United States cannot combat illicit finance or stop terrorist financing alone.

In a November 12, 2023, Wall Street Journal article, it describes the use of cryptocurrency——specifically *international* exchanges——by Hamas, but it also describes their use of global investment portfolio, raising money through charitable organizations (which has previously been shown to be done by terrorist organizations prior to 9/11, and skimming off funds from official foreign aid and tax revenues in Gaza."[82] The use of the foreign exchanges for terrorist activity suggests that lawmakers must consider how to collaborate with international counterparties to prevent illicit actors from jurisdictional arbitrage[83] that jeopardizes U.S. efforts to combat terrorist financing.

---

79 *Id.*

80 *See* Angus Berwick and Ian Talley, *Hamas Militants Behind Israel Attack Raised Millions in Crypto*, The Wall Street Journal (Oct. 10, 2023), https://www.wsj.com/world/middle-east/militants-behind-israel-attack-raised-millions-in-crypto-b9134b7a.

81 *Id.*

82 *See* Angus Berwick and Ian Talley, *Hamas Needed a New Way to Get Money From Iran. It Turned to Crypto*, The Wall Street Journal (Nov. 12, 2023), https://www.wsj.com/world/middle-east/hamas-needed-a-new-way-to-get-money-from-iran-it-turned-to-crypto-739619aa; Rory Jones, Ian Talley, and Benoit Faucon, *How the West—and Israel Itself—Inadvertently Funded Hamas*, The Wall Street Journal (Oct. 19, 2023), https://www.wsj.com/world/middle-east/hamas-gaza-humanitarian-aid-diverted-cf356c48.

83 2020 Cryptocurrency Enforcement Framework, *supra* note 1 at 56.

Hawalas

In my experience investigating financial crimes and money laundering case, it is more difficult to trace money where individuals use *hawalas,*[84] black market peso exchanges,[85] or trade-based money laundering than when an investigator traces digital assets on a public blockchain. *Hawalas* allow transfers of funds outside conventional banking systems and often rely on trust between community members, non-bank financial institutions, and in some cases, handwritten or manual reporting of how much money was transferred and to whom, and can be done crossborder.[86] When I was investigating human trafficking and human smuggling networks at DOJ,[87] there were illicit massage business networks using cash,[88] *hawalas,*[89] and trade-based money laundering from Africa, Middle East and Southeast Asia.[90] Unlike digital assets on the blockchain, following the money when defendants were using *hawalas* was incredibly challenging, time consuming, and often constrained law enforcement ability to seize assets. Moreover, some foreign jurisdictions where *hawalas* are more commonly used are less cooperative and may not respond to U.S. MLAT requests or other legal process.

Despite the disputed data on how terrorist organizations may be using digital assets to fund their criminal activity, it is critical to find effective ways to curb terror finance. It is also clear that if terrorist organizations are using foreign exchanges, the United States cannot combat

---

84 FinCEN, Advisory: Issue 33, *Informal Value Transfer Systems* (March 2003), https://www.fincen.gov/sites/default/files/advisory/advis33.pdf ("An 'informal value transfer system' refers to any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. The transfers generally take place outside of the conventional banking system through non-bank financial institutions or other business entities whose primary business activity may not be the transmission of money.").

85 Press Release, U.S. Attorney's Office, Southern District of Texas, *Six Convicted for Roles in Multi-Million Dollar Black Market Peso Exchange Money Laundering Scheme* (Feb. 12, 2019), https://www.justice.gov/usao-sdtx/pr/six-convicted-roles-multi-million-dollar-black-market-peso-exchange-money-laundering.

86 Advisory: Issue 33, *supra* note 84.

87 *E.g.,* Press Release, U.S. Attorney's Office, District of Minnesota, *Thirty-Six Defendants Guilty For Their Roles In International Thai Sex Trafficking Organization* (Dec. 13, 2018), https://www.justice.gov/usao-mn/pr/thirty-six-defendants-guilty-their-roles-international-thai-sex-trafficking-organization.

88 *See, United States v. Kyong Burgos*, No. 18-CR-126 (S.D. Miss.); *see also See United States v. Michael Morris, et al., No. 17-CR-107 (D. Minn. 2017); United States v. Sumalee Intarathong, et al., No. 16-CR-257 (D. Minn. 2017); United States v. Peter Griffin et al., 22-CR-1828 (S.D. Cal. 2022) (*https://www.justice.gov/usao-sdca/pr/former-san-diego-police-officer-and-three-others-sentenced-crimes-stemming-years-long).

89 Advisory: Issue 33, *supra* note 84 ("An 'informal value transfer system' refers to any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form.").

90 Thirty-Six Defendants Guilty*, supra* note 87.

illicit finance or stop terrorist financing alone, but that also does not mean that lawmakers should prohibit all use of blockchain technology.

IV. Importance of Digital Asset Ecosystem to Protect the Vulnerable from Oppressive Regimes, Authoritarian Leaders, and Maintaining U.S. National Security Interests

Digital assets and blockchain technology can often be the only access available to the most vulnerable and a protection of democratic ideals.

Ukraine Relief

We also must allow the most vulnerable to be supported. Over two years ago, when Russia invaded Ukraine, thousands of innocent civilian Ukrainian citizens lost access to funds. My family scrambled to assist friends and family in cities like Odesa, Kherson, Nikholai, and elsewhere. Onerous sanctions and compliance processes of traditional financial institutions and money transmitter businesses caused weeks-long delays in processing payments leaving many civilians and refugees with limited to no access to necessary funds. In fact, in the European Union, the European Banking Authority had to publish a statement to ensure traditional financial institutions and supervisors ensured access to Ukrainian refugees for at least basic financial products and services.[91]

On the other hand, data suggests that cryptocurrency, including Bitcoin and Ether,[92] were critical to supporting the Ukrainian people.[93] According to Alex Bornyakov, Ukraine's deputy minister at the Ministry of Digital Transformation, Ukraine raised $100 million in crypto after soliciting donations.[94] This aid was possible because cryptocurrency can be transferred instantaneously, cross-border, and directly to the people who need it the most and may not be

---

[91] European Banking Authority, *EBA Calls on Financial Institutions and Supervisors to Provide Access to the EU's Financial System* (April 27, 2022), https://www.eba.europa.eu/eba-calls-financial-institutions-and-supervisors-provide-access-eu-financial-syst .em; *See also*, Zofeen Ebrahim, *Afghan Refugees Fear Return as Pakistan Cracks Down on Migrants*, ReliefWeb (Feb. 1, 2023), https://reliefweb.int/report/pakistan/afghan-refugees-fear-return-pakistan-cracks-down-migrants.

[92] Elliptic Threat Intel, *Live Updates: Ukraine Government Turns to Crypto to Crowdfund Millions of Dollars*, Elliptic (March 11, 2022), https://www.elliptic.co/blog/live-updates-millions-in-crypto-crowdfunded-for-the-ukrainian-military.

[93] *Id.*; Ananya Kunar and Nikhil Raghuveera, *Can Crypto Deliver Aid amid War? Ukraine Holds the Answer*, Atlantic Council (April 4, 2022), https://www.atlanticcouncil.org/blogs/new-atlanticist/can-crypto-deliver-aid-amid-war-ukraine-holds-the-an swer.

[94] Amitoj Singh, *Ukraine Has Received Close to $100M in Crypto Donations*, CoinDesk (May 11, 2023), https://www.coindesk.com/business/2022/03/09/ukraine-has-received-close-to-100-million-in-crypto-donati ons/.

able to get to a bank. The ability to reduce scam risk of vulnerable communities with real-time verification of the flow of digital assets during times of crisis is key.[95]

Humanitarian Relief and Aid to Human Rights Defenders

In the aftermath of the heinous and barbaric terrorist attack by Hamas on civilians in Israel, U.S.based company Fireblocks, which assists digital asset projects with compliance, helped establish a relief fund for displaced Israelis and humanitarian aid.[96] In addition, after the Taliban took over governmental control in Afghanistan, local communities and civilians lost access to bank accounts, cash, and ways to receive funds from abroad, so they turned to digital assets.[97] Unfortunately, in response to civilians turning to digital assets in order to maintain control over their lives and financial independence, the Taliban banned cryptocurrency and called Bitcoin fraudulent.[98] In recent months, human rights organizations in the United States have also struggled to get financial aid to human rights defenders in Afghanistan because similar to my family's experience with Ukraine, traditional financial options are no longer available or will be too costly.

Access to Financial Institutions for Vulnerable Population

I also believe that using new and emergent technology in a thoughtful manner is critical to the United States' ability to secure its national security interests at home and abroad. During my tenure at the DOJ, I interviewed dozens of survivors of human trafficking and learned how our traditional financial systems can deprive them of tools to reenter society, obtain education and employment, and thrive in the community.

The growth of blockchain technology has helped reduce costs and give communities access to basic financial services. According to UNICEF, 31% of adults globally are unbanked, and cannot access basic financial services.[99] Through the use of tools in the digital asset ecosystem, unbanked users can borrow capital or earn interest in savings without having to utilize a traditional banking institution. UNICEF is partnered with UC Berkeley to explore the

---

95 *See* United Nations Office on Drug and Crime, *Conflict in Ukraine: Key Evidence on Risks of Trafficking in Persons and Smuggling of Migrants*, UNODC (December 2022), https://www.unodc.org/documents/data-and-analysis/tip/Conflict_Ukraine_TIP_2022.pdf.

96 *See* Margaux Nijkerk, *Israel War Prompts Crypto Firms Including Fireblocks, MarketAcross to Start Aid Fund*, CoinDesk (Oct. 9, 2023), https://www.coindesk.com/tech/2023/10/09/israel-war-prompts-crypto-firms-including-fireblocks-marketacross-to-start-aid-fund/; Crypto Aid Israel, https://cryptoaidisrael.com/.

97 Anamaria Silic, *Afghans Turn to Cryptocurrencies amid US Sanctions*, BBC News (March 16, 2022), https://www.bbc.com/news/world-asia-60715707.

98 Eltaf Najafizada, *Taliban Ban Crypto in Afghanistan, Arrest Dealers of Tokens*, Bloomberg (August 26, 2022), https://www.bloomberg.com/news/articles/2022-08-26/taliban-ban-crypto-in-afghanistan-arrest-digital-coin-dealers.

99 Mehran Hydary and Christina Lomazzo, *Generating Income to Benefit Communities*, UNICEF Office of Innovation (August 12, 2021), https://www.unicef.org/innovation/stories/generating-income-benefit-communities.

growing potential of the technology.[100] In addition, during a time of high unemployment for youth in Kenya during COVID-19, MercyCorps. and Celo Foundation partnered with NairoBits to train 200 Kenyan youth to have access to digital microwork from global platforms - using a mobile app and integrating their wallet on the blockchain.[101] Helping empower youth and provide infrastructure in a meaningful and democratic way will help the United States combat the national security risks that will be described below.

V. Combating Illicit Finance through Cross Border Collaboration and Protecting to National Security

The United States should continue to support and allow innovation to flourish while tailoring current regulatory frameworks to continue to combat anti-money laundering and terrorist financing. I believe lawmakers should ensure that compliant U.S.-based companies and projects using digital assets are not pushed out of the country and into regimes that have more opaque legal and financial safeguards, which could undermine America's national security interests.

China

China leverages traditional and emergent financial systems to further its interests. For example, evidence related to the DOJ's seizure of $11 million from corporations used by North Korea to circumvent sanctions showed that certain corporations were incorporated in China.[102] As technology evolves, China has evolved its approach to digital technology to its advantage. Even after China cracked down on Bitcoin mining in 2021, the Chinese government has leaned into innovation in the digital asset space. Last year, Chinese state-owned banks participated in a trial focused on cross-border transactions developed by the Bank of International Settlements.[103] China is also actively digitizing the yuan.[104] Hong Kong, which is now under Chinese control, has also leveraged uncertainty toward digital assets by the United States to partner with large,

---

100 *Id.*

101 Celo Foundation, *Pilot Spotlight: How Celo and Mercy Corps Ventures Partnered to Benefit Microworkers in Kenya,* The Celo Blog (Feb. 22, 2022), https://blog.celo.org/pilot-spotlight-how-celo-and-mercy-corps-ventures-partnered-to-benefit-microworkers-in-kenya-882dc767aee.

102 Press Release, U.S. Attorney's Office, District of Columbia, *United States Files Complaints to Forfeit More Than $11 Million From Companies That Allegedly Laundered Funds To Benefit Sanctioned North Korean Entities* (August 22, 2017), https://www.justice.gov/usao-dc/pr/united-states-files-complaints-forfeit-more-11-million-companies-allegedly-laundered.

103 Jason Xue and Brenda Goh, *China Trials Cross-Border Settlement Involving Cenbank Digital Currencies,* Reuters (September 29, 2022), https://www.reuters.com/markets/currencies/china-trials-cross-border-settlement-involving-cenbank-digital-currencies-2022-09-29.

104 Rae Wee, *China's Digital Yuan Transactions Seeing Strong Momentum, says CBank Gov Yi*, Reuters (July 19, 2023), https://www.reuters.com/markets/asia/chinas-digital-yuan-transactions-seeing-strong-momentum-says-cbank-gov-yi-2023-07-19.

global institutions, to explore green bonds and smart contracts.[105] If the U.S. does not stay ahead or at least keep up with China's use of new technology, that could put the U.S. at both an economic and national security disadvantage.

It is also important to note that after the passage of the Uyghur Forced Labor Protection Act (UFLPA)[106] in 2021 and its enforcement starting in June 21, 2022[107]——which aims to identify, detain and seize shipments of goods from Xinjiang Uyghur Autonomous Region of the People's Republic of China——the U.S. Customs and Border Protection has denied[108] $67,690,123 from China alone.[109] I believe lawmakers should consider whether this law could be more effective if CBP and U.S. corporations used blockchain to trace the source of goods and services.

Russia

When Russia invaded Ukraine in February 2022, many questioned whether Russia would evade sanctions through the use of digital assets. While some said the Russian Federation would try to use all financial tools and natural resources at their fingertips, the traceability of Bitcoin and other digital assets, and lack of robust liquidity makes it difficult to achieve that objective. However, Russia has capitalized on the use of blockchain technology, and like China, has digitized the ruble.[110] Russia has also established centralized exchanges to help launder funds for

---

105 BIS Innovation Hub, *Genesis 2.0: Smart Contract-Based Carbon Credits Attached to Green Bonds*, Bank of International Settlements (October 23, 2022), https://www.bis.org/about/bisih/topics/green_finance/genesis_2.htm.

Prarthana Prakash, *As America Obsesses over ChatGPT, It's Losing the Race with China on Tech in 37 out of 44 Key Areas, Study Funded by the State Department Says*, Fortune (March 2, 2023), https://fortune.com/2023/03/02/tech-race-china-us-stunning-western-democracies-losing-ai-quantum-state-department.

106 Public Law No. 117-78.

107 U.S. Customs and Border Protection, *Uyghur Forced Labor Prevention Act* (July 21, 2023), https://www.cbp.gov/trade/forced-labor/UFLPA.

108 U.S. Customs and Border Protection, *Uyghur Forced Labor Prevention Act Statistics* (October 21, 2023), https://www.cbp.gov/newsroom/stats/trade/uyghur-forced-labor-prevention-act-statistics.

109 *Id.*; Annual Testimony of the Secretary of the Treasury, *supra* note 11.

110 Ananya Kumar and Charles Lichfield, Russia Is Ramping Up Its CBDC. Will Putin's 'Robot Ruble' Work?, Atlantic Council (August 29, 2023), https://www.atlanticcouncil.org/blogs/new-atlanticist/russia-is-ramping-up-its-cbdc-will-putins-robot-ruble-work.

their allies, like Iran,[111] and continued to attempt to circumvent sanctions,[112] in order to further advance their foreign policy objectives against the free world.

If the United States allows China and Russia and others to harness new technology only for nefarious purposes, the detrimental consequences to democratic ideals and national security risks could be catastrophic.

Strengthening Collaboration with International Bodies and Allies

We live in a global world where the internet, cross border payments, and finance are not confined to the digital asset space. Cross-border collaboration is critical to close gaps or prevent jurisdictions with poor or no regulatory frameworks to take advantage of our financial systems.[113]

Cross-border law enforcement cooperation has led to successful investigations and prosecutions of criminal networks using digital assets. In October 16, 2019, the DOJ indicted the owner and operator of Welcome to Video, a darknet child pornography website that was the largest online child sexual exploitation market at the time of the DOJ's seizure.[114] This case involved global coordination of law enforcement including IRS-CI, HSI, the National Crime Agency in the U.K., and the Korean National Police in South Korea, who together helped identify the wallet addresses of at least 337 users of the website through the use of blockchain data.[115] In March 12, 2020, the DOJ used blockchain evidence to take down "Darkscandals," another website that featured child abuse material.[116] Related to that same case, the government filed a civil forfeiture action seeking recovery of illicit funds from 303 virtual currency accounts allegedly used by customers to fund DarkScandals and to promote child exploitation.[117]

---

111 Berwick et. al., *supra* note 82.

112 *See* 2020 Cryptocurrency Enforcement Framework, *supra* note 1 ("Rogue states like Russia, Iran, and North Korea may turn to cryptocurrency to fund cyber-attacks, blunt the impact of U.S. and international sanctions, and decrease America's influence in the global marketplace.").

113 *See* 2020 Cryptocurrency Enforcement Framework, *supra* note 1 at 10.

114 Press Release, U.S. Department of Justice, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin* (October 16, 2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child.

115 *Id.*

116 Press Release, U.S. Attorney's Office, District of Columbia, *Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 'Real Rape' and Child Pornography Videos, Funded by Cryptocurrency* (March 12, 2020), https://www.justice.gov/usao-dc/pr/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child.

117 *Id.*

In November 2020, at the FATF Joint Expert's Meeting, I presented best practices in following the money and asset recovery, including cases involving digital assets.[118] This was an incredibly valuable opportunity for experts around the world to share information, successes and failures, and joint paths forward for collaboration around the same topics we are addressing here: international legal frameworks to prevent illicit finance, terrorist financing, and advancing digital transformation (including privacy preserving technology) and how technology could increase efficiency in identifying and disrupting suspicious activity.[119]

The DOJ's 2020 Cryptocurrency Enforcement Framework also advocates for close collaboration with international partners to effectively investigate and prosecute cases involving virtual currency.[120] Given the July 2023 FATF call on more jurisdictions to implement the Travel Rule to close loopholes for criminal networks suggests that more cross border collaboration is necessary. The small number of jurisdictions implementing current FATF guidance may also be why illicit crime is occurring through overseas entities.

As such, lawmakers in the U.S. should work as they have with partners abroad like the U.K., European Union, and others, to be on the forefront of closing the jurisdictional arbitrage that foreign actors are currently exploiting not only in the digital asset space but across the financial sectors. It is clear that failure by actors abroad to comply with AML/CFT could jeopardize the U.S. and the entire international financial system much beyond the digital asset ecosystem. Coordinated efforts and international cooperation among regulators will be necessary to effectively address regulatory challenges in this space. The objective should be to achieve minimum global standards, supported by cross-border cooperation and information sharing across jurisdictions, to help ensure optimal consistency.

CONCLUSION

The United States must stay at the forefront of innovation to ensure democratic values are preserved while being measured and deliberate about what steps are necessary to preserve national security interests. Blockchain technology is not inherently good or bad. Blockchain technology can be used to more effectively trace supply chains, prevent fraud in government procurement, provide access to vulnerable populations to financial independence, digital identity, and much more.

The U.S. also has a robust anti-money laundering and countering terrorist financing legal and regulatory framework. It is critical that these laws are used to detect, disrupt, and dismantle criminal organizations and networks. I urge lawmakers to ensure that the nexus between blockchain and global affairs is seen in the nuanced context that emerging technology brings.

Thank you again for the opportunity to participate in this conversation. I am grateful to be able to share my personal and professional experiences to ensure that the U.S. continues to be

---

[118] Financial Action Task Force, *Joint Meeting of Experts 23-26 November 2020* (November 26, 2020), https://www.fatf-gafi.org/en/publications/Methodsandtrends/Jem-2020.html.

[119] *Id.*.

[120] 2020 Cryptocurrency Enforcement Framework, *supra* note 1 at 61.

at the forefront of innovation, a beacon of hope for the most vulnerable, and a staunch ally against the abhorrent actions of autocratic regimes and terrorist organizations.