TESTIMONY OF

Carole House[1]

BEFORE THE

United States House Financial Services Committee

Subcommittee on Digital Assets, Financial Technology, and Inclusion

Hearing on Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity

February 15, 2024

Thank you Chairman Hill, Ranking Member Lynch, and distinguished members of the Subcommittee, for holding this hearing and the honor of the invitation to testify on combating illicit activity in digital assets. I applaud your leadership in convening the Subcommittee on this important issue. I hope my testimony will be helpful in considering some of the most important aspects of cryptocrime, as you navigate the incredibly complex issues at play here relating to security, innovation, and personal liberty.

Issues of national, economic, and technological security have affected many aspects of my life and ultimately shaped my approach toward cryptocurrency illicit finance. My father taught me to don my chemical protective mask in nine seconds when I was twelve years old. I had just moved with my family to the Republic of Korea, where dependent families of U.S. servicemembers were issued gas masks to wear in the case of a chemical attack by North Korea. That moment underscored to me the dangers presented by a rogue nation and the far-reaching, tangible consequences that escalated conflict with them could bring – the simple fact that I was a child and noncombatant would not save me from a gruesome threat once unleashed. And these consequences reached far beyond me, endangering my family, neighbors, strangers, the country I was living in, and my home nation. This is the unfortunate reality of many of the grave threats presented by rogue nations and transnational organized crime that persist today. Like many of those here today, I joined the government because I wanted to do something about it.

I pursued a career focused at the intersection of national security, emerging technologies, and finance. I served as an Army officer in chemical defense and military intelligence, and then in civilian life worked at the White House Office of Management and Budget's (OMB) newly created Cyber and National Security Unit and the Senate Homeland Security and Governmental Affairs Committee (HSGAC) working on policy aimed at combating illicit exploitation of technology and cyber threats. From there I moved to FinCEN, where I led cyber, virtual currency, and digital identity policy efforts.

[1] Nonresident Senior Fellow, Atlantic Council GeoEconomics Center; Executive in Residence, Terranet Ventures, Inc.; Senior Research Scholar, Georgetown University. Advisory Roles: Chair, Commodity Futures Trading Commission Technology Advisory Committee; Advisory Board Member, Third Way U.S.-China Digital World Order Initiative; Advisory Board Member, Digital Dollar Project; Senior Advisor, FS Vector. Previous Roles: Director of Cybersecurity and Secure Digital Innovation, White House National Security Council; Senior Strategic Policy Officer for Cyber and Emerging Technology, U.S. Financial Crimes Enforcement Network; Presidential Management Fellow (PMF) and Policy Advisor, White House Office of Management and Budget and U.S. Senate Homeland Security and Governmental Affairs Committee; Captain, U.S. Army.

FinCEN provided an optimal vantage point to understand the nature of malicious activity like ransomware as inherently dual-natured as a *cyber*crime and a *financial* crime, with both technological and financial infrastructure presenting specific vulnerabilities being exploited as well as levers available for disruption. I also gained a deep appreciation of the critical role that industry plays in security frameworks like cybersecurity and countering illicit finance – policy and regulations do not work if they are not implemented. The strength and integrity of our financial and tech sectors ultimately place the United States in a highly advantageous position to reach our goals of detecting and countering threats. I carried these insights with me as I served on the White House National Security Council (NSC) as the Director for Cybersecurity and Secure Digital Innovation, where I helped plan, coordinate, and drive key initiatives like the U.S. Counter-Ransomware Strategy and President Biden's Executive Order on Ensuring Responsible Development of Digital Assets. Currently at both Terranet Ventures[2] and the Atlantic Council, I continue to conduct research and advise industry and policymakers on issues critical for the future of secure and trustworthy digital economies, including cybersecurity, identity, anti-money laundering, digital assets and DLT, and AI/ML.

Innovation sits at the heart of the U.S. economy, essential to how we generate jobs and grow new industries, and preserve global economic leadership and competitiveness. However, responsible innovation does not mean unchecked technological advancement without regard to implications for society, security, and democratic values. Cryptocurrency remains a serious risk for illicit finance. It is not inevitable for the sector to always be that way, but the existing state of compliance domestically and abroad across the industry have cultivated an environment ripe for exploitation by rogue nations and fraudsters. There are mitigating measures as well that are helping us to combat illicit finance, but critical steps are needed to make best use of them. The status quo has not yielded benefits for consumers, the evolving DeFi ecosystem, or U.S. leadership in financial services and technology.

Areas for action that can help better place agencies, international partners, and the industry to detect and combat illicit finance include (1) enhancing regulatory and enforcement capability to take action against egregious violators of our illicit finance framework, (2) promoting international action on combating illicit cryptocurrency activity, (3) enhancing outcome-oriented public-private partnerships for information sharing, and (4) promoting development of secure, trustworthy, and interoperable digital identity solutions and infrastructure.

Threat Overview: Cryptocurrency Exploited in Illicit Finance

Key Features of Cryptocurrency and Associated Risks

Before discussing the type and amount of illicit cryptocurrency activity, it can be helpful to examine how key features of crypto can enhance or mitigate risks for specific assets. As emphasized in a recent report Commodity Futures Trading Commission (CFTC) Technology Advisory Committee

[2] Terranet Ventures is a research and advisory firm supporting projects in the fields of distributed ledger technologies (DLT), cybersecurity, quantum, central bank digital currencies (CBDCs), artificial intelligence and machine learning (AI/ML), and others in a variety of ways, ranging from direct investment to providing operational expertise, to incubation of solutions, to contributing as technical and strategy advisors.

(TAC)[3], "the benefits and risks of [decentralized finance (DeFi)] depend significantly on the design and features of specific systems." These systems can vary widely given thousands of cryptocurrencies with a reported total market cap of $1.87 trillion.[4] However, there are several key features that generally pertain to most cryptocurrencies.

Core to cryptocurrency's appeal is its ability to transfer significant value **peer-to-peer** (i.e., from user to user without the need for a typical custodial role of a third-party financial intermediary), **pseudonymously**, **immutably** (or irreversibly), with **global reach**, with **increased speed and cost efficiencies**.[5] These features that make cryptocurrency attractive to licit users also make it attractive to illicit users to send criminal proceeds anywhere in the world at lower cost and friction. While many of these features also exist in the traditional finance and payment systems, *they generally do not co-exist at the same time all in one instrument or system*. For example, cash movements can be peer-to-peer and pseudonymous, but generally take significant time and space to move globally, and wire transfers can have global reach but require the use of regulated intermediary financial institutions to transfer the funds. This aggregation of higher-risk features can increase the illicit finance risk profile of cryptocurrencies, especially if controls to lower risk (such as anti-money laundering and countering financing of terrorism [AML/CFT] requirements like "know your customer" [KYC], reporting, and recordkeeping) are not in place. And these controls are typically not in place sufficiently, as AML/CFT compliance is lagging significantly across the sector internationally.[6]

The **absence or reduction of financial institution intermediaries and central points of control** in more highly decentralized cryptocurrency systems also removes many of the key points where mitigating controls would typically be implemented. While Treasury has long maintained the position that most entities that claim to be decentralized remain either highly or somewhat centralized, identifying the specific entity for accountability can be challenging and time-consuming. This disintermediation can present one of the clearest challenges to combating illicit finance and consumer exploitation in that it can *obscure clear lines of responsibility and accountability* within cryptocurrency ecosystems. With this absence of clear responsible parties, compounded by the immutability or unchangeability of cryptocurrency ledgers, it can be extremely challenging to provide mechanisms for victim recourse as well as timely adaptation to take measures to stop movement of illicit funds or patch security vulnerabilities in networks and smart contracts.[7]

One important distinction between most cryptocurrency systems and traditional financial systems is cryptocurrency's often **public and transparent nature** – SWIFT, FedWIRE, and cash movements do not publish transactions to public ledgers or records that anyone can see.

---

[3] I served as co-chair with Cornell University's Dan Awrey of the TAC Subcommittee on Digital Assets and Blockchain Technology. *See* CFTC TAC Subcommittee on Digital Assets and Blockchain Technology, Report, "Decentralized Finance," (January 2024).

[4] *See* CoinMarketCap, website (last accessed February, 12, 2024).

[5] Security consultant Alison Jimenez described these features as ability to move funds "far, fast, in large amounts, irreversibly, anonymously, and to a third party." *See* Alison Jimenez, written testimony to House Financial Services Committee Subcommittee on Digital Assets, Financial Technology, and Inclusion, Hearing on Crypto Crime in Context-Breaking Down the Illicit Activity in Digital Assets (November 15, 2023).

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

[7] *See* CFTC TAC Subcommittee on Digital Assets and Blockchain Technology, Report, "Decentralized Finance," (January 2024).

Cryptocurrency systems offer unprecedented public visibility of certain financial activity. This public visibility has played an important role in mitigating risks in cryptocurrency illicit finance, enabling the rise of cryptocurrency analytics firms and investigative tools and techniques to better and more timely trace and interdict crypto crime proceeds.[8] However, there are limitations to this transparency, such as in that off-chain data and transactions are not visible[9], as well as the use of methods like mixing, chain-hopping, and encryption to obscure the ledger or system of record.[10] There are also disagreements amongst analytic firms on attributions made using proprietary analytic methods and AI/ML clustering models, as well as ongoing concerns with auditability, corroboration, explainability of some of these proprietary solutions that could present serious challenges to best leveraging what information is public on blockchain ledgers.[11] Public transparency of financial information also inherently presents challenges for consumer privacy, especially when considering the pace of open source AI/ML technologies that may increase public attribution of transactions on unobscured ledgers.

(*See Appendix A for a more detailed description of key pros and cons for common cryptocurrency features.)*

Cryptocurrency Illicit Finance

While it is difficult to accurately assess the amount of illicit finance in any financial system, including in cryptocurrency ecosystems, regulatory technology (RegTech) firms as well as financial and law enforcement networks shed some light on the scale of the problem. Some analytics firms estimate less than **1%** of cryptocurrency transaction volume to be illicit,[12] However, while these and other RegTech firms are critical to enable investigations by industry and law enforcement, this figure and others from blockchain analytics firms likely underestimate illicit activity. While the figures would represent best estimations from the firms based on information available to them, the numbers would not be comprehensive. They would not account for off-chain data and only include activity already known to the RegTech firms as having been identified to be illicit. In 2020, FinCEN highlighted that it received suspicious activity reporting (SARs) in 2019 associated with cryptocurrency activity amounting to $119 billion, or **11.9%** of the total cryptocurrency market.[13] Of course, this number may likely be overestimated, as "suspicious" activity does not mean it is necessarily illicit. However, the FinCEN SAR figure also only accounted for reporting from *compliant, U.S. cryptocurrency service providers*, implicating that global suspicious activity metrics would be much higher, especially if global compliance were in a better state to address pervasive underreporting issues.

Just as with fiat currencies, there are a wide array of methods where criminals and rogue nations are exploiting vulnerabilities in cryptocurrency, ranging across cybercrime, proliferation financing,

---

[8] *See* United States District Court for the District of Columbia, Case No. 20-sw-314 (ZMF), *In the Matter of the Search of One Address in Washington, D.C., Under Rule 41* (January 6, 2021).
[9] For example, this could include internal cryptocurrency exchange activity or transactions conducted off-chain over the Bitcoin Lightning Network via a Lightning channel.
[10] *See* FinCEN, Advisory FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019).
[11] *See* Ciphertrace, Defense Expert Report, *United States v. Roman Sterlingov*, *21-CR00399 (RDM)* (August 8, 2023).
[12] *See* Chainalysis, "2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth" (January 18, 2024).
[13] *See* FinCEN, 85 FR 83840, Notice of Proposed Rulemaking, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (December 23, 2020).

fraud and scams, sanctions evasion and offset, narcotics and human trafficking, and terrorism financing. For criminals, the absence of sufficient regulatory controls like KYC provisions, the irreversible nature of transactions, and the speed of movement and conversion of cryptocurrencies make them attractive as a means of payment and laundering. They also recognize cryptocurrency as an attractive target to (1) hack due to platforms' often poor cybersecurity, and (2) entice victims with the appeal of potential involvement in what seems to be a profitable market.

Cybercrime. Cryptocurrency remains cybercriminals' favored means of payment and laundering, to include for purchases of digital servers, bulletproof hosting, and use of virtual private networks (VPNs) used in the conduct of their malicious cyber activity.[14]

- *Hacks and Cyber-enabled Theft* – Poor cybersecurity and the high value nature of cryptocurrency platforms have presented enticing targets for cybercriminals aiming to steal funds. Between 2011 and 2020, exchange hacks resulted in over $15 billion worth of cryptocurrency being stolen[15], not to mention the additional economic costs to the industry in recovery costs and reputational damage. DeFi exploits are also significant, targeting of security weaknesses or code errors in smart contracts, DeFi protocols, and cross-chain bridges. Cross-chain bridge hacks and thefts amounted to approximately $2 billion in 2022 alone.[16] DeFi platforms are also reportedly growing as the destination of funds leaving identified illicit wallets, and were the top destination by far of stolen cryptocurrency.[17]

- *Ransomware* – Ransomware remains a significant threat targeting U.S. critical infrastructure, serving as a pervasive form of *disruptive* cybercrime extorting Americans and businesses – especially enterprises connected to critical infrastructure such as energy and healthcare – by denying them access to their systems or confidentiality of their data unless they pay up. While ransomware has existed in some form since 1989, the emergence of cryptocurrencies as an easy means for nearly-instantaneous cross-border value transfer with limited traceability[18] contributed to the rise of sophisticated Ransomware-as-a-Service economies as lucrative illicit business models.[19] In 2023, identified ransomware payments reportedly hit a record high of over $1 billion.[20] In 2021, FinCEN received reporting of at least 1,251 ransomware-related incidents amounting to approximately $886 million, with Russian-related ransomware variants responsible for 75% of reported ransomware incidents.[21] Ransomware activities generally involve largely or entirely illicit actors, like crypting service providers, cryptocurrency mixers, darknet

[14] *See* EUROPOL, Spotlight Report, "Cryptocurrencies: Tracing the Evolution of Criminal Finances" (2021).
[15] *See* Crystal Blockchain and Cointelegraph, Magazine by Cointelegraph, "Report on Crypto Exchange Hacks" (2023).
[16] *See* TRM Labs, "Illicit Crypto Ecosystem Report" (June 2023).
[17] *See* Chainalysis, "Crypto Crime Report 2023" (February 2023).
[18] Note that while cryptocurrencies were inaccurately perceived as untraceable, the continued absence of sufficient AML/CFT compliance globally as well as growth of a spectrum of increasingly sophisticated methods of obfuscation like use of mixers, anonymity-enhanced cryptocurrencies like Monero, and chain-hopping have kept cryptocurrency systems in their current state still valuable for use by ransomware criminals.
[19] *See* Kurt Baker, Crowdstrike, "History of Ransomware" (October 10, 2022).
[20] *See* Chainalysis, Blog, "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline" (February 7, 2024).
[21] *See* FinCEN, Financial Trend Analysis, "Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021" (November 1, 2022).

markets, and malware providers, as well as exploitation of generally licit actors, like antivirus vendors, cryptocurrency exchanges, and hosting and VPN services providers.[22]

- *Proliferation Financing via Cybercrime* – The Biden Administration reported that North Korea funds about half of its missile program via cybercrime and cryptocurrency theft.[23] United Nations sanctions monitors are reportedly at the time of this hearing investigating over 58 suspected North Korean cyberattacks amounting to over $3 billion between 2017 and 2023 in support of its nuclear proliferation program and in direct contravention of international sanctions.[24]

Fraud and Scams. Frauds and scams in crypto have taken many different forms, with one report estimating over $9 billion in fraud schemes in 2022.[25]

- *Investment Fraud* – In 2022, the Federal Bureau of Investigation (FBI) observed cryptocurrency investment fraud schemes targeting victims with fake investment opportunities rose 183% from $907 million in 2021 to $2.57 billion. These scams ranged from fraudulent liquidity mining applications, schemes broadcast over hacked social media accounts, and celebrity impersonations.[26]

- *Pig Butchering and Romance Scams* – "Pig butchering" is on a the rise, a type of scam where the criminal develops a relationship with the victim and then pressures them to invest in fake investment platforms, often conducted through offers of romance and initiated on dating apps, social media sites, or text messages purported to have inadvertently been sent to a wrong number.[27] These scams can be absolutely devastating to victims, resulting in significant economic losses. In one instance of scammers targeting five victims for a total loss of over $10 million, law enforcement seized the domains used by the scammers, which were spoofs of the Singapore International Monetary Exchange.[28]

The Consumer Financial Protection Bureau (CFPB) reported in their analysis of consumer complaints in 2022 that 40% of the 8,300 complaints they received associated with cryptocurrency listed frauds and scams as their complaint. They also noted a significant increase in reports from older consumers, indicative of increasing trends of elder exploitation using cryptocurrency.[29]

Sanctions Evasion and Offset. Cryptocurrencies are also being used to varying extents by rogue nations and sanctioned actors as part of broader strategies to evade and offset the impact of sanctions regimes. Crypto-heists perpetrated by the North Korean state-sponsored Lazarus Group are also an example of sanctions evasion to generate revenue for the North Korean regime.

---

[22] *See* Zoe Brammer, Institute for Security and Technology, "Mapping Threat Actor Behavior in the Ransomware Payment Ecosystem: A Mini-Pilot" (May 2023).
[23] *See* Sean Lyngaas, CNN, "Half of North Korean Missile Program Funded by Cyberattacks and Crypto Theft, White House Says" (May 10, 2023).
[24] *See* Michelle Nicols, Reuters, "Exclusive: UN Experts Investigate 58 Cyberattacks Worth $3 Bln by North Korea" (February 8, 2024).
[25] *See* TRM Labs, "Illicit Crypto Ecosystem Report" (June 2023).
[26] *See* FBI, Internet Crime Complaint Center (IC3), "Internet Crime Report 2022" (March 2022).
[27] *See* U.S. Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023).
[28] *See* U.S. Department of Justice, U.S. Attorney's Office (USAO), Eastern District of Virginia, "Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency 'Pig Butchering' Scheme" (November 21, 2022).
[29] *See* CFPB, "Complaint Bulletin: An Analysis of Consumer Complaints Related to Crypto-assets" (November 2022).

Another method of offset involves cryptocurrency mining, essentially enabling sanctioned actors to leverage energy resources in generation of cryptocurrency that can gain them access to global crypto financial markets. For example, Iran-based miners are estimated to account for 4.5% of all Bitcoin mining, meaning Iran is "effectively selling its energy reserves on the global markets, using the Bitcoin mining process to bypass trade embargoes essentially enabling Iran to convert its oil reserves."[30]

In October 2022, the U.S. Department of Justice (DOJ) charged two Venezuelan and five Russian nationals as criminal enablers to Russian oligarchs, specifically for their use of shell companies, bulk cash, and cryptocurrency to evade sanctions and export controls to acquire Venezuelan oil and U.S. military technology.[31] However, it is important to note that in the case of countries under significant sanctions like Russia, limited liquidity in cryptocurrency markets and low adoption rates of crypto in exchange for goods and services make cryptocurrency a difficult primary vehicle for a state's-worth of sanctions evasion.[32]

Drug Trafficking. Cryptocurrency is growing as part of a suite of tools for broader transnational organized crime groups like cartels, whose use of cryptocurrency has grown 450% to $27 million among companies suspected of involvement in fentanyl trafficking, an amount analytics firm Elliptic assessed to facilitate purchase of enough precursor to produce $54 billion worth fentanyl pills.[33]

Human Trafficking and Child Sexual Abuse Material (CSAM). Cryptocurrency along with mobile payments are increasingly used in human trafficking. For example, GAO found that 15 of 27 analyzed online commercial sex marketplaces accepted cryptocurrencies.[34] The FBI has also warned the public about cyberscamming schemes leveraging forced labor and human trafficking victims to commit international investment fraud schemes. In these cases, the victims are drawn to a foreign country with promises of lucrative benefits and salaries, then held against their will and forced through intimidation and extortion to engage in these frauds.[35] CSAM vendors also often rely on cryptocurrency for payment and laundering, and are also increasing their sophistication with use of mixers and anonymity-enhanced cryptocurrencies (AECs) like Monero to obfuscate their movements of funds and evade law enforcement.[36]

Terrorism Financing. Cryptocurrencies have been used as a tool in financing of terrorism, though as one of many tools used by terrorist groups along with their primary methods like use of fiat currency and hawala networks.[37] The FATF reported in 2023 the increasing risk

[30] *See* Elliptic, 2023 Report, "Sanctions Compliance in Cryptocurrencies" (2023).
[31] *See* USDOJ, USAO, Eastern District of New York, "Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme" (October 19, 2022).
[32] *See* Government Accountability Office (GAO), GAO-24-106178, "Economic Sanctions: Agency Efforts Help Mitigate Some of the Risks Posted by Digital Assets" (December 2023).
[33] *See* Elliptic, Elliptic Research, "Chinese Businesses Fueling the Fentanyl Epidemic Receive Tens of Millions in Crypto Payments" (May 23, 2023).
[34] *See* GAO, WatchBlog, "As Virtual Currency Use in Human and Drug Trafficking Increases, So Do the Challenges for Federal Enforcement" (February 24, 2022).
[35] *See* FBI, Public Service Announcement, I-052223-PSA, "The FBI Warns of False Job Advertisements Linked to Labor Trafficking at Scam Compounds" (May 22, 2023).
[36] *See* Chainalysis, Blog, "CSAM and Cryptocurrency: On-chain Analysis Suggests CSAM Vendors May Benefit from Privacy Coins like Monero and Other Obfuscation Measures" (January 11, 2024).
[37] *See* Audrey Alexander and Teddy MacDonald, Combating Terrorism Center (CTC) at West Point, *Sentinel*, vol 15 (3), "Examining Digital Currency Usage by Terrorists in Syria" (March 2022).

cryptocurrencies pose to terrorism financing, such as through various sources and jurisdictions reporting that ISIL, Al Qaeda, and affiliates continue to use cryptocurrencies to raise and move funds in Africa, Europe, and the Middle East, as well as use by right-wing extremist groups. The FATF report also noted that that the vast majority of terrorism financing still occurs using fiat currency.[38]

Other National Security Concerns. The United States derives significant national and economic security benefits from the central role we play in the global financial system and international trade. This central role of the U.S. and our currency as the global reserve provides a foundation and multiplier of our ability to wield geopolitical power and influence abroad. Despite this importance, the United States is lagging in experimentation with certain digital assets like central bank digital currencies (CBDCs), DeFi, and DLT infrastructure, while adversarial nations pursue joint experimentation on alternative financial systems, as well as on infrastructure like China's Blockchain Services Network (BSN) that aims to set the foundation for the next phase of the internet.[39] New developments in financial systems could in the medium- to long-term present potential changes to aspects of the existing system like corresponding banking relationships, which could carry significant implications for sanctions and AML/CFT frameworks.

While there may not be a near-term threat to the United States and the dollar's central role, it is critical to be deliberate in ensuring that our economic framework, including that for cryptocurrencies and DLT, preserves and reinforces U.S. leadership in financial system and technological infrastructure developments so as not to open the door in the long term to geopolitical competitors that may challenge U.S. leadership in these realms. Increased experimentation

Counter-Illicit Finance Frameworks Applied to Cryptocurrency

Frameworks for countering illicit finance should be risk-based, whole-of-nation approaches that have weighed the benefits and burdens to achieve an appropriate balance of achieving desired outcomes without disproportionate or unacceptable costs on privacy, liberty, and resources. These frameworks are critically important to nations and societies, establishing a foundation to better detect and prevent critical national security threats and enable recourse once someone is exploited or defrauded. Ultimately, an effective AML/CFT framework is the only way for digital assets to attain the consumer trust needed to drive mass adoption.

A whole-of-nation approach embraces the concept that neither government nor industry can accomplish our desired ends of mitigating illicit finance on our own. The government cannot scale to subsidize or enforce a sector into AML/CFT compliance and responsible development without partnership from cooperative actors in industry, audit, and compliance firms, and industry participants like financial institutions rely on the government to provide guidance and guardrails, as well potential partnership through areas like liability protections and sensitive information

[38] *See* FATF, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 2023).
[39] *See* Yaya Fanusie, United States Congress U.S.-China Economic and Security Review Commission, written testimony, Hearing on An Assessment of the CCP's Economic Ambitions, Plans, and Metrics of Success Panel IV: China's Pursuit of Leadership in Digital Currency (April 15, 2021).

sharing. The FATF framework accounts for the whole of the nation; mutual evaluations of jurisdictions' frameworks assess both industry as well as government legal, regulatory, supervisory, law enforcement, financial intelligence unit (FIU), prosecutorial, and judicial authorities for compliance with the FATF Recommendations.[40]

U.S. Domestic Policy Coverage and Compliance to Combat Cryptocurrency Illicit Finance

Policy. The U.S. illicit finance framework for cryptocurrencies is the oldest and most comprehensive framework in the world. U.S. regulatory, law enforcement, and FIU capabilities for AML/CFT have been tip of the spear for years, and placed the U.S. delegation I participated in to play a critical role in shaping the FATF virtual asset standards. The Bank Secrecy Act (BSA), the backbone of the U.S. illicit finance framework and primary AML/CFT statute, has covered most cryptocurrency business models like exchanges and administrators as money services businesses (MSBs) under its regulations since at least 2011 and via clarifying Guidance in 2013 and 2019.[41] Entities like unhosted (or self-custodied) wallet providers and miners are generally not covered, though in my view, Treasury has some broad authorities to expand the definition of financial institution[42] to incorporate such entities if it wishes.[43]

Our sanctions framework administered by the Office of Foreign Assets Control (OFAC) under the International Emergency Economic Powers Act (IEEPA) applies not just to U.S. financial institutions but instead to all U.S. persons and on a strict liability standard to not engage in prohibited transactions with sanctioned persons or jurisdictions. OFAC has published guidance highlighting that actors like U.S. miners, which may not be regulated as MSBs but still play certain roles in transactions, such as in validation, *may* have sanctions screening obligations.[44]

Enforcement. The United States has been a global leader in enforcement against illicit actors in the cryptocurrency space, including significant enforcement actions like penalties against BTC-e, Bittrex, and against Binance, the largest cryptocurrency exchange in the world.[45] OFAC has levied many sanctions designations involving illicit cryptocurrency actors and has even brought a few enforcement actions against exchanges for sanctions violations. However, enforcement actions have generally been on extended timelines at a slower pace due to complexity and difficulties of investigations compounded by insufficient agency resourcing. Treasury has also been subject to significant litigation consistently when it uses its authorities, which increases the

---

[40] *See* FATF, "Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems" (October 2023).
[41] *See Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011).
[42] *See* 31 U.S.C. (a)(2)(Y).
[43] Additionally, other areas where cryptocurrency financial institutions or activity are not treated with parity to comparable fiat activity or traditional institutions (e.g., Financial Bank Account Report [FBAR] holdings at foreign cryptocurrency exchanges, or creating a version of an equivalent report for high-value disintermediated cryptocurrency transactions to the cash reporting requirements of currency transaction reports [CTRs] or 8300s) appear clearly within Treasury's regulatory authority to put in place, once their resources permit and their risk-based approach calls for it.
[44] *See* OFAC, Guidance, "Sanctions Compliance Guidance for the Virtual Currency Industry" (October 2021).
[45] *See* U.S. Department of the Treasury FinCEN, No. 2017-03, In the matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik (July 26, 2017); Treasury, "Treasury Announces Two Enforcement Actions for Over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc.," (October 11, 2022); *and* U.S. Department of the Treasury FinCEN, No. 2023-04, IN the Matter of Binance Holdings Limited, Binance (Services) Holdings Limited, Binance Holdings (IE) Limited, d/b/a Binance and Binance.com.

resource commitment required for each enforcement action. Additionally, while FinCEN has used its enforcement and designation authorities under sections 311 and 9714, both face potential limitations to their use that could be addressed to enhance their use against bad actors.

Compliance. Compliance across the cryptocurrency sector remains challenged and inconsistent even in the U.S. where regulations have been in place for over a decade. Many do not implement sufficient frameworks to identify their customers, and others claim not to be subject to U.S. jurisdiction. Still yet others do not meet critical requirements to mitigate risk when dealing with higher risk assets like AECs. On the whole, issues with compliance are resultant from choices by the people and businesses behind the platforms rather than because of the technology.

In the absence of sufficient compliance with AML/CFT standards internationally, policymakers have turned their eyes to DeFi to see if there are actions that should be taken to address illicit finance risks presented by this largely disintermediated activity that is growing as a preferred destination of funds out of illicitly-connected wallets. Where discernible entities were identified, agencies like the CFTC have taken action against DeFi actors like in the recent OokiDAO case.[46] Many have called for policymakers to exclusively focus on on-and-off ramps for regulation. Such exchanges are certainly useful given their visibility and proximity to the customer, but ultimately as and if DeFi is more widely adopted and cryptocurrency used in exchange for goods and services, the reliance on on-and-off ramps is insufficient where much of the activity moves outside of them. Regulating beyond on-and-off ramps maya be necessary if illicit finance risks are not sufficiently mitigated by focusing frameworks on exchanges. In that case, policymakers may need to assess what reshaping AML/CFT and other illicit finance obligations should look like elsewhere in the "DeFi technology stack." At each "layer" of DeFi ecosystems, there are different options for players or components to focus obligations on and potential features or controls that could help meet regulatory objectives.

[46] *See* CFTC, No. 8590-22, "CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act" (September 22, 2022).

Figure 1. *Potential Mechanisms to Support Security and Compliance throughout the DeFi Tech Stack*[47]

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

U.S. Government Efforts Supporting the Whole of Nation Approach. The Biden Administration and agencies continue to drive ongoing prioritization and efforts focused on combating illicit finance in cryptocurrency. For example, the International Counter-Ransomware Initiative (CRI) launched in 2021 continued to meat, with an entire prong of international collaboration with 50 nation partners committed to addressing illicit finance risks. This past November, the CRI announced capacity building and training efforts as well as an initiative to create a shared blacklist of wallets, led by Treasury's sharing of information on wallets associated with ransomware actors.[48] Agencies continue to fight to prevent and disrupt North Korean cryptocurrency heists.[49] The FBI-chaired National Cyber Investigative Joint Task Force (NCIJTF) is also partnering with Treasury to build a public-private partnership called the Illicit Virtual Asset Notification (IVAN) partnership.[50]

International Policy Coverage and Compliance to Combat Cryptocurrency Illicit Finance

Almost 5 years after adoption of the FATF Standards for virtual assets, more than half of jurisdictions have not taken steps to implement the Travel Rule (a crucial element to an effective

[47] Table with illustrative examples of compliance as possible, taken from CFTC TAC DeFi Report.
[48] *See* White House, "International Counter Ransomware Initiative 2023 Joint Statement" (November 1, 2023).
[49] *See* U.S. Treasury, Press Release, "Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency" (November 29, 2023).
[50] *See* White House, "Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware" (October 13, 2021).

AML/CFT framework to help counterparty institutions understand the risk exposure of their activities).[51] Where policy is not yet in place, enforcement and compliance internationally inherently lag. This issue of jurisdictional arbitrage presents significant challenges for U.S. authorities' abilities to combat illicit activity to moves without regard to international borders. A security firm focused on asset recovery operations and capacity building recently testified to UK Parliament about the significant challenges across the Global South, where there are higher levels of cryptocurrency adoption but also weaker infrastructure and capacity, to combat illicit finance in cryptocurrency: "These are global asset recovery challenges. Where there is more adoption of crypto in general, there is an inherently higher risk: if you swim in those waters, you will meet more predators."[52] Greater focus on capacity building and enhancing political will to address cryptocurrency illicit finance is needed globally.

Key Issues for Consideration

Privacy

Privacy is consistently raised as a critical point of concern in cryptocurrency ecosystems, and rightfully so. Privacy is an important democratic value critical to support security, human autonomy, and dignity. Considering how to approach privacy demands an honest intellectual accounting of the needs of relevant stakeholders and the technical, operational, and governance implementations that can achieve the desired balance and end state.

In the cryptocurrency community where financial activity is posted publicly and unencrypted on an open ledger, there are real concerns about how to preserve desirable privacy while still maintaining the benefits that transparency of ledgers provide for blockchain's security and trust models. Keeping this in mind, I would like to share some views on some of the key points I hear on privacy that may be helpful to you as you consider what level of privacy you find permissible within cryptocurrency environments:

- **Distinction between Privacy and Anonymity.** First, there are some voices who speak about privacy in a way that really appears to be intimating *anonymity*, generally the idea that one's identity should not be discoverable to anyone under any circumstances. Privacy is not quite the same thing as anonymity – instead, privacy doesn't mean the absence of data, it typically means the present of sensitive, protected data that can be discovered or disclosed under established permissions, protections, and conditions. It can be useful to consider carefully in your approach (1) what information should be discoverable (2) by whom and (3) under want conditions. These choices will ultimately inform the governance and tech infrastructure put in place.

- **Collection and Sharing of Originator and Beneficiary Information (ref. Travel Rule).** There are some proponents who advocate against requiring cryptocurrency financial institutions from collecting identity information about customers and the beneficiaries of

[51] *See* Financial Action Task Force (FATF), "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 27, 2023).
[52] *See* Aidan Larkin, Asset Reality, UK Parliament Joint Committee on the National Security Strategy, oral evidence, "Ransomware" (April 24, 2023).

funds transfers, and then potentially sharing the information about the counterparties with any receiving crypto exchange as part of compliance with the FATF Travel Rule (or the U.S. transfer and travel rules). Arguments against these provisions are typically based on privacy concerns, stating that collection of personally identifiable information (PII) will just create a honeypot for cybercriminals to steal. Policymakers should consider whether institutions that claim that they should not be expected or trusted to secure sensitive data should be trusted to securely custody customer financial assets. The information required under the travel rule is generally consistent with identify information one would need to understand their potential sanctions and illicit finance exposure.

Internet Corollary and Credible Neutrality

There are also many in industry calling for treating cryptocurrency systems or specific components, such as underlying "layer 1" infrastructure, like we do the internet. Specifically, that means to some to approach DeFi as we do internet service providers (ISPs) under the principle of net neutrality, somewhat adapted for cryptocurrency contexts under a concept of "credible neutrality."[53] This concept requires earnest debate and examination – in my view it may not be an "either/or" choice between financial institution of some kind or infrastructure provider, but instead be a "yes, and" for certain platforms, given the dual nature of this infrastructure to service as inherently financial but also to support non-financial applications.

DeFi infrastructure essentially provides the underlying rails for both financial and information or communications activity. Those are two very different types of activity with differing types of regulations, high value nature, and expectations of privacy versus identity discoverability. Those who want the maximum privacy reserved for information activities naturally want the internet framework of neutrality imposed. However, *I am not convinced that achieves desirable outcomes for society – over 200 member jurisdictions of the FATF, which the United States helped establish under the G7, have all agreed that "neutrality" is not an acceptable position to take toward illicit finance.* It may work as an approach if risks are sufficiently mitigated elsewhere within the ecosystem, but the current state of compliance in the industry globally is not yet encouraging. At present, I suspect that internet-equivalent and information activity will need to be treated differently in areas like privacy and neutrality than certain kinds of economic activity where we demand greater protections and accountability.

- **DeFi as Infrastructure.** In the CFTC TAC report on DeFi, we discussed the idea that DeFi elements may likely meet certain definitions of infrastructure providers that will be affected by policies such as two ongoing rulemakings: (1) the Cybersecurity and Infrastructure Security Agency's (CISA's) upcoming proposed rules under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) that will require *critical infrastructure* operators to report significant cyber incidents[54], and (2) the Department of Commerce's proposed rulemaking imposing KYC and other requirements on Infrastructure-as-a-Service (IaaS) providers.[55]

[53] *See* Vitalik Buterin, Nakamoto, "Credible Neutrality as a Guiding Principle" (January 3, 2020).
[54] *See* the Cyber Incident Reporting for Critical Infrastructure Act of 2022.
[55] See Department of Commerce, 86 FR 5698, Notice of Proposed Rulemaking, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities" (January 29, 2024); and

Recommendations

Getting the framework right to combat illicit finance in cryptocurrency is critical. The technology is not inherently evil or useless, though haphazard implementation of these systems can create an environment where DeFi platforms and exchanges can operate as open ATMs to take over half a billion dollars per hack in support of the worst national security threats facing the globe. We can do better as a nation, and we *must* demand more of the international community to drive timely, responsible development in this space.

In pursuit of this belief that we can do better, I will respectfully offer some recommendations for consideration by the Subcommittee on what could help combat crypto-enabled illicit finance:

- **Pursue sustained domestic and international enforcement and disruption as early as practical, prioritized against the most egregious violators.** The U.S. AML/CFT policy regime has covered cryptocurrency for the longest in the world and quite comprehensively since at least 2011. The greatest challenges in cryptocurrency illicit finance are the most part not generally *policy* weaknesses, but instead are about insufficient *implementation* of existing obligations, either through failures in compliance for U.S.-operating companies, though that is improving; insufficient agency resources and capacity to drive timely, scaled enforcement; and especially the absence of sufficient regulation and enforcement abroad hindering investigations. Enforcement earlier in the extremely fast-paced lifecycle of these companies will better shape those institutions and the broader sector with less costly adjustments down the road, and will also reward more compliance actors in the space who end up waiting, calling for actions that can take many years all the while the illicit actor benefits from lesser compliance than the licit actors.

  To accomplish this, Congress could consider the following –

  - Provide funding, resources, and innovative hiring and acquisitions authorities, consistent with certain cyber authorities, that can enable government agencies to build their capacity and competencies on cryptocurrency and illicit finance.

  - Engage agencies in development of strategies and requirements to scale amount, impact, and timeliness of enforcement and disruption of crypto illicit finance activity. Engage OFAC about the extent of compliance obligations and enforcement or implementation approach toward "network layer" participants like miners and validators. Prior to pursuing regulation of these participants as new financial institutions, it may be prudent to drive compliance and enforcement of already-existing obligations for them regarding validation of transactions to designated actors before adding new requirements.

  - Support FinCEN's completion of the 311 "of primary money laundering concern" designation on mixed cryptocurrency transactions based on feedback from the

President Biden's Executive Order 14110, "Executive Order on the Safe, Secure, Trustworthy Development and Use of Artificial Intelligence" (2023).

public comment period. Engage FinCEN on its plan to meaningfully use the information collected.

- Hone FinCEN's disruption authorities to better disrupt illicit actors and threats using cryptocurrency beyond those exclusively Russia-related, and clarify application to just illicitly operating non-banking financial institutions. Specifically, adjust FinCEN's 9714 designation authority to apply beyond just Russian-related illicit finance, which would allow this special designation authority to be able to be used against other threats of concern, such as Iran, North Kora, and Hamas[56], and adjust FinCEN's 311 designation authority to explicitly confirm FinCEN's ability to use it regarding cryptocurrency activity.[57] Also consider the authorities requested by Treasury on enhancing its ability to fight terrorism financing in cryptocurrency, many of which help clarify and defend against litigation of use of existing authorities while others propose significant expansion.

- Prioritize passing of comprehensive stablecoin legislation to establish a comprehensive prudential regulatory regime with a clear path to registration and strong illicit finance and prudential requirements and oversight.

- **Promote international action on combating cryptocurrency illicit finance.** The United States cannot police illicit actors in this space on our own, especially given the highly distributed and cross-border nature of most of these operations. We were successful in establishing the policy framework, implementation lags. Now almost five years after the standards were adopted, 75% of jurisdictions are only partly or not compliant with the FATF virtual asset standards.[58]

  Policymakers should consider the most effective way to step into driving tangible progress in implementation of the FATF standards across priority jurisdictions, to make effective use of limited resources:

  - Direct the development and resourcing of agency strategies for driving accelerated implementation of the FATF Standards, leveraging combinations of diplomatic pressure and capacity building across their top priority jurisdictions, based on factors like hosting the largest, most non-compliant, or most maliciously operating exchanges.

- **Enhance outcome-oriented public-private partnerships and information sharing.** Significant amounts of illicit activity in cryptocurrency are detected on public, unobscured ledgers. Not that we would want to, but we should be *able to* dare criminals to launder on a public ledger and be confident in our ability to catch the actor and prevent successful movement of their funds, but we are not yet there. The conditions of the technology have long been ripe for setting up the infrastructure and partnerships to enable real-time operational information sharing across licit actors in the ecosystem to enable real-time, even machine-readable sharing of illicit cryptocurrency indicators in the same vein that cybersecurity indicators have long been shared across industry. With 314(b) liability

[56] *See* section 9714(a) of the Combating Russian Money Laundering Act (Public Law 116-283), as amended by section 6106(b) of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81).
[57] *See* 31 U.S.C. 5318A.
[58] *See* Financial Action Task Force (FATF), "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 27, 2023).

protections[59] provided to cryptocurrency financial institutions to share illicit finance information, and Cybersecurity Information Sharing Act liability protections[60] to U.S. industry to share cyber threat indicators and defensive measures, while there are some measures that could enhance them and try to address their underutilization, the stage is well set to enable information sharing.

There are several existing public-private partnership efforts sitting at varying degrees of maturity focused on combating illicit finance, to include IVAN, the Crypto-Information Sharing and Analysis Center (ISAC) that is being launched, the National Cyber Forensics Training Alliance (NCFTA), FinCEN's Rapid Response Program (RRP), and the FBI's Financial Fraud Kill Chain (FFKC) program. There could be opportunities to resource and scale these efforts to accelerate high-impact progress with industry. Steps that may help support these and other public-private partnership efforts:

- Resource and direct agencies to establish, enhance, and accelerate countering illicit finance partnerships to engage in real-time information sharing and interdiction of illicit cryptocurrency proceeds.

- Strengthen and promote use of existing liability protections like those under 314(b) for illicit finance and the Cybersecurity Information Sharing Act for cybercrime. For example, consider adjusting the 314(b) information sharing liability protection to more closely mirror that of the Cybersecurity Information Sharing Act, which has achieved greater scale of adoption despite being passed by Congress almost 15 years later. Specifically, consider whether expansion of the 314(b) information sharing liability protection to include *financial service providers*, rather than just financial institutions, to better meet 314(b)'s intent to drive better detection and prevention of illicit finance. In the example of cryptocurrency activity, financial services or RegTech firms like the blockchain analytics companies are generally not also financial institutions, and therefore are likely ineligible for the liability protection despite the fact that they are often best placed to see early warning of illicit finance movements. In comparison, all private entities, to include cyber threat firms, are covered under the Cybersecurity Information Sharing Act.

- Engage with key stakeholders, whose role in the cryptocurrency ecosystems could drive far-reaching impacts, to determine a way forward on development and implementation of standards and best practices for issues like accountability, due diligence, built-in dynamic compliance, and security in DeFi. For example, consider whether there are opportunities to partner with high-impact members of the ecosystem in the investment community, the major platforms and network participants, and the top research and development (R&D) and academic institutions

- **Promote development of secure, trustworthy, and interoperable digital identity solutions and infrastructure.** While there is experimentation ongoing in cryptocurrencies and "web3" about how to integrate digital identity into the systems, most of the efforts are not addressing the core challenges that exist with identity even in the traditional system. Without deliberate action, the cryptocurrency system may inadvertently

[59] *See* FinCEN, "Section 314(b) Fact Sheet" (December 2020).
[60] *See* CISA, "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance" (October 15, 2021).

just import the broken elements of traditional identity into web3, a system with less accountability and recourse for victims. Example measures that could benefit the cryptocurrency digital identity ecosystem include[61]:

- Providing funding and mandates for Federal grants to support development and issuance of standards-compliant mobile driver's licenses and other verifiable credentials.
- Direct NIST, DHS, and other agencies to accelerate development of standards and guidance to states on remote identity proofing applications for digital credentials.
- Establish consent-based attribute validation services across agencies that hold authoritative identity information on Americans in support of identity ecosystems that could combat fraud in web3.
- Resource and accelerate NIST's efforts to develop more robust guidance and criteria for liveness detection in biometrics to enable defenders to fend off deepfakes.

In closing, I'd like to again underscore my gratitude for the opportunity to speak with you all today. Meaningful engagement like this is the only way to ensure that our democratic principles and policy objectives shape the future of money and this space to protect consumers and the integrity of our financial system.

Thank you.

[61] These recommendations are derived from the Better Identity Coalition's recent published report, "Better Identity at Five Years: An Updated Blueprint for Policymakers" (January 2024).

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

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

Figure 2. Potential Pros and Cons for Combating Illicit Finance Presented by Key Features of Cryptocurrency[62]

Feature Description	Potential Pro	Potential Con
Decentralization – The extent to which the system has no single point of failure, does not rely on a single source of information, and is not governed by a central authority that is capable of altering or censoring this information. Generally will manifest across *functional* dimensions (e.g., access, development, governance, balance sheet, operational) and technological dimensions (e.g., open source software, smart contracts, etc.) of decentralization.	With greater decentralization, a system may exhibit greater operational resilience against manipulation by illicit actors like cybercriminals aiming to take over a network. A more decentralized system can also mitigate "too-big-to-fail" concentration risks and potentially enable greater competition in the marketplace.	With the removal or reduction of key intermediaries in high-risk, high-value activity, decentralization can challenge the ability to identify clear lines of responsibility and accountability for when things go wrong or to implement fixes to security vulnerabilities or recover stolen or illicit funds.[63] Fewer intermediaries can also reduce points for detection and interdiction of illicit activity.
Speed and Cost Efficiencies – The ability to transfer funds and financial assets quickly and with lower costs, generally driven through optimizing aspects like automation, network capacity, and reducing or consolidating intermediaries.	Licit actors and consumers benefit from an alternative to existing systems like slow and costly cross-border remittances.[64]	Efficiencies in cost and speed can also increase for illicit actors, enabling their ability to scale frauds and money laundering at lower cost and friction.
Openness and Global Reach – The extent to which a system permits participants into the ecosystem and movement of assets anywhere in the world. "Permissionless" systems generally implement no restrictions to those who can access the system, while permissioned systems implement some type of control on ecosystem participation.	Can lower barriers to financial access for the 1.7 billion people around the world who are unbanked[65], and (if the system is sufficiently regulated and appropriately transparent) could enhance the ability to detect illicit activity within an observable ecosystem.	With unrestricted openness can enable access for illicit actors like rogue states who are otherwise restricted from the global financial system. Level of tech savvy also presents remaining barriers to entry and broader adoption. With inadequacies in consumer protection and regulation, open systems could enable "predatory inclusion."[66]

[62] These illustrative summaries leverage descriptions from the CFTC TAC report on DeFi. *See* CFTC TAC Subcommittee on Digital Assets and Blockchain Technology, Report, "Decentralized Finance," (January 2024)
[63] *See* Osato Avan-Nomayo and Aislinn Kelly, The Block, "Circle Freezes USDC Funds in Tornado Cash's US Treasury-Sanctioned Wallets" (August 8, 2022).
[64] *See* The World Bank, "Remittance Prices Worldwide Quarterly: An Analysis of Trends in Costs of Remittance Services" (March 2023).
[65] *See* The World Bank, "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19" (June 2022).
[66] *See* Tressie McMillan Cottom, "Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society", 6:4 Sociology of Race and Ethnicity 441 (October 2020).

Transparency – Includes the nature and amount of information (such as critical information needed to understand risks like for counterparties, sanctions, screening, etc.) that is available, whether publicly or some means of disclosure, to ecosystem participants. Public, unobscured blockchains generally have a lot of information about the existence, amount, provenance, and destination of transactions that is visible to the public.	The high level of transparency of most cryptocurrency ledgers enables detection, monitoring, and investigation of cryptocurrency illicit finance, often more efficiently than traditional investigations.[67]	Much of the raw data available cannot be effectively used by investigators due to issues of capacity, resources, or insufficient RegTech. The transparency of public ledgers is insufficient without additional AML/CFT measures, as they only include information that is "on-chain," not "off-chain" transaction and identity information. Transparency also presents significant privacy concerns, and is also not inevitable. Obscuring methods through use of anonymity-enhanced cryptocurrencies, mixers, and other privacy enhancing technologies (PETs) are already used, and likely to be integrated at greater scale.
Pseudonymity and Anonymity – The ability to conduct transactions without one's identity being known or discoverable.	Licit users can engage in more private financial activity without needing to disclose sensitive personal information that could be a target for illicit actors.	This pseudonymity, without compensating AML/CFT controls like KYC measures and some form of discoverable identity elsewhere in the ecosystem, denies critical information for investigators and for counterparties to understand the nature of the risk of their counterparty.
Immutability and Censorship Resistance – The inability of network participants to change a system's ledgers, protocols, transactions, or other features.	Assets can be used to provide financial support to populations under repressive regimes via means the regime cannot interdict and deny access to.[68] Could promote greater auditability and resilience to manipulation by illicit actors in the financial system.	With increased immutability brings increased challenges to censor illicit actors and activities on a network. It also is more difficult to implement desired changes to a system, such as to patch a software vulnerability or recover assets stolen due to a security weakness.

[67] *See* Ari Redbord, written testimony to the U.S. House Committee on Financial Services Subcommittee on National Security, International Development, and Monetary Policy, Hearing on Under the Radar: Alternative Payment Systems and National Security Impacts of their Growth (September 20, 2022).
[68] *See* Circle, blog, "Circle Partners with Bolivarian Republic of Venezuela and Airtm to Deliver Aid to Venezuelans Using USDC" (November 20, 2020).