MEMORANDUM

To: Republican Members, Committee on Financial Services

From: Financial Services Republican Staff

Date: November 13, 2023

Re: Subcommittee on Digital Assets, Financial Technology, and Inclusion Hearing: "Crypto Crime in Context: Breaking Down Illicit Activity in Digital Assets"

On Wednesday, October 25, 2023, at 10:00 a.m. (ET), the Subcommittee on Digital Assets, Financial Technology, and Inclusion will hold a hearing entitled: "Crypto Crime in Context: Breaking Down Illicit Activity in Digital Assets." The following witnesses will testify:

Witnesses:

- Bill Hughes, Senior Counsel & Director of Global Regulatory Matters at ConsenSys and previously Associate Deputy Attorney General at the Department of Justice
- Jane Khodarkovsky, Partner at Arktouros and previously Trial Attorney and Human Trafficking Finance Specialist with the U.S. Department of Justice's Money Laundering and Asset Recovery Section
- Jonathan Levin, Co-Founder & Chief Strategy Officer, Chainalysis
- Gregory Lisa, Chief Legal Officer, DELV (f/k/a Element Finance, Inc.) and Senior Counsel, Hogan Lovells US LLP. Previously Interim Director, Office of Compliance and Enforcement at Financial Crimes Enforcement Network
- Alison Jimenez, President, Dynamic Securities Analytics, Inc.

Blockchain Technology and Digital Assets

One value proposition that blockchain networks and the digital assets that transact on top of them offer is that there is a transparent and immutable record of all transactions that have and will occur. Any transaction on one of these networks can be identified by a public address that is linked to the wallet where the transaction originated. Thus, any individual with access to the internet can look up a given blockchain network and view the entire transaction history of a public address. An entire subindustry within the digital asset ecosystem has developed to analyze public blockchains, determine trends in activity, and support law enforcement in rooting out illicit activity. Blockchain analytics firms, in partnership with law enforcement in the United States and abroad, have made considerable progress in helping to reduce illicit activity.

Another feature of blockchain networks is the public nature and ease of access. While increased accessibility contributes to increased consumer engagement, it also means increased access by bad actors. While it is inevitable that criminals will look to new and evolving mechanisms, like digital assets, to fund their illicit activity, the amount of illicit activity relative to the amount of licit activity is minimal.[1] This point was confirmed by the Department of Treasury when it acknowledged that "most virtual currency activity is licit."[2] To ensure that the digital asset ecosystem is not exploited by bad actors, it is critical that Congress understand the degree to which illicit activity exists, what tools are available to combat this activity and explore any potential gaps to prevent and detect illicit activity.

Estimated levels of illicit activity in the digital asset ecosystem

Money Laundering

According to the Treasury Department's 2022 National Money Laundering Risk Assessment, "the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods."[3] Nevertheless, bad actors may seek to use digital wallets, mixers, and digital asset trading platforms to transact and obfuscate the movements of digital assets. Importantly, the exchange of illicitly obtained digital assets for fiat removes the ability for law enforcement to trace the transaction that would otherwise be available through blockchain.[4] Treasury has highlighted that the problem is not with the United States but with digital asset platforms that operate outside of the U.S. that have "substantially deficient" anti-money laundering programs. Treasury has emphasized that "uneven and often inadequate regulation and supervision internationally allow virtual asset service providers (VASPs) and illicit cyber actors to engage in regulatory arbitrage and expose the U.S. financial system to risk from jurisdictions where regulatory standards and enforcement are less robust."[5]

Terrorist Financing

Considerable focus has been placed on terrorists' use of digital assets to fund their operations. While there has been increased attention on the use of digital assets, it still pales in comparison

[1] Chainalysis 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking (Jan. 23, 2023), *available at* https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/.
[2] U.S. Department of the Treasury, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange," (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471.
[3] U.S. Department of the Treasury, "National Money Laundering Risk Assessment," (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf, pg. 41.
[4] Chainalysis, "The 2023 Crypto Crime Report," (Feb. 2023), https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf
[5] U.S. Department of the Treasury, "National Money Laundering Risk Assessment," (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf, pg. 41.

to the use of traditional financial assets by terrorists. Indeed, Treasury's 2022 National Terrorist Financing Risk Assessment concluded that "the vast majority of terrorist funds raised in the United States still move through banks and money transmitters or are in cash."[6]

AML/CFT Considerations in Digital Assets

The AML/CFT regime for the United States' financial system is predicated on the existence of regulated intermediaries. These intermediaries are not present in certain parts of the digital asset ecosystem. As a result, there is considerable ambiguity on how and if the United States' AML/CFT laws apply to certain parts of the digital asset ecosystem. For example, while centralized exchanges, stablecoin issuers and other entities are considered financial institutions under the Bank Secrecy Act, there are other facets of the ecosystem that do not have a readily identifiable entity to apply the requirements of the BSA. Notwithstanding this ambiguity, the majority of illicit activity in the digital asset ecosystem does occur outside of U. S., in less regulated or non-compliant jurisdictions.[7]

Exchanges and Other Centralized Digital Asset Operations

Centralized exchanges, stablecoin issuers, and other entities are subject to BSA obligations which include: registering with FinCEN; developing, implementing, and maintaining an effective AML program; filing suspicious activity reports (SARs) and currency transaction reports (CTRs); appointing a chief compliance officer; conducting training; and maintaining certain records.[8] In addition, entities are responsible for monitoring their platforms and blocking any users that are on OFAC's Sanctioned Designated National List or from a sanctioned jurisdiction.

Decentralized Finance (DeFi)

DeFi refers to a class of digital asset protocols and platforms that allow for automated P2P transactions without the need for an account or custodial relationship with a third-party. These protocols and platforms are open to anyone with an internet connection.[9] Law enforcement has

---

[6] U.S. Department of the Treasury, "2022 National Terrorist Financing Risk Assessment," (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf, pg. 22.
[7] U.S. Department of the Treasury, "National Money Laundering Risk Assessment," (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment, pg. 41.
[8] Bank Secrecy Act, 31 U.S.C. §§ 5311-5336 (2023)
[9] DeFi users seeking to cash out of the digital asset ecosystem (i.e. exchange their digital assets for fiat) can only do so at centralized intermediaries. For illicit actors using DeFi, this means that they might be able to move their funds within the digital asset ecosystem (i.e. from blockchain to blockchain), which is visible to anyone with an internet connection, including law enforcement, but they will not be able to exchange them for goods or services unless they go through a centralized intermediary where KYC requirements are in place. At that point, law enforcement can work with the centralized "off-ramp" to identify the illicit actors.

reported an increase in illicit activity involving DeFi. [10] Specifically, law enforcement investigations involving digital assets have uncovered chain hopping (moving assets from one blockchain network to another) facilitated via smart contracts and other DeFi services. Because individual users interact with a DeFi protocol on their own to conduct a financial activity, they retain custody and control over their assets throughout the transaction. The lack of an entity behind the protocols raises questions about BSA's applicability.

According to Treasury's Illicit Finance Risk Assessment of Decentralized Finance, "illicit activity is a subset of overall activity within the DeFi space and, at present, the DeFi space remains a minor portion of the overall virtual asset ecosystem. Moreover, money laundering, proliferation financing, and terrorist financing most commonly occur using fiat currency or other traditional assets as opposed to virtual assets."[11]

Law Enforcement Actions in the Digital Asset Ecosystem

FinCEN

FinCEN has brought several enforcement actions involving certain digital asset firms. In October 2020, FinCEN charged a founder of two mixers, Helix and Coin Ninja, for operating unregistered MSBs and "implement[ing] practices that allowed Helix to circumvent the BSA's requirements."[12] In August 2021, the agency assessed a civil money penalty against BitMEX, a digital asset derivatives exchange, for "willful violations of the BSA."[13] Further, in October 2022 FinCEN brought action against Bittrex, a digital asset exchange and licensed money services business, for the same violation. In January 2023, FinCEN identified Russian digital asset exchange, Bitzlato, as "a primary money laundering concern" in connection with Russian illicit finance, which the agency determined was a "serious threat" to the United States' economy and national security.[14]

OFAC

---

[10] U.S. Department of the Treasury, "National Money Laundering Risk Assessment," (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment, pg. 42.
[11] *Id,* pg. 36.
[12] FinCEN, "First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws," (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.
[13] FinCEN, "FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act." (Aug. 10, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures.
[14] FinCEN, "FinCEN Identifies Virtual Currency Exchange Bitzlato as a "Primary Money Laundering Concern" in Connection with Russian Illicit Finance," (Jan. 18, 2023), https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering.

OFAC has taken numerous actions against sanctions evaders attempting to use the digital asset ecosystem.[15] The first action occurred on November 28, 2018, when OFAC designated two Iran-based individuals who executed an elaborate ransomware scheme and demanded ransom payments in Bitcoin.[16] Since that first designation, OFAC has included many digital wallet addresses and even entire digital asset services in its designations. For example, OFAC has sanctioned three virtual currency exchanges, Suex, Chatex, and Garantex, as well as the largest darknet market in the world, Russia-based Hydra.[17] OFAC has also taken steps to counteract one of North Korea's cybercrime groups, the Lazarus Group, including sanctioning two digital asset mixers, Blender.io and Tornado Cash, that were used by North Korea to process their ill-gotten gains as well as Chinese nationals that helped North Korea launder funds following attacks on several digital asset exchanges.[18]

Department of Justice (DOJ)

The Department of Justice both issues enforcement actions against criminals operating in the digital asset ecosystem as well as conducts seizures of illegally obtained digital assets. In April 2023, the DOJ seized an estimated $112 million linked to digital asset romance scams.[19] In February 2022, the agency arrested two individuals and seized over $3.6 billion in digital assets linked to a 2016 hack of the digital asset exchange, Bitfinex. Additionally, in June 2021, approximately $2.3 million dollars worth of Bitcoin was seized from the proceeds of the May 8, 2021, Colonial Pipeline hack that resulted in portions of the United States' critical infrastructure being taken out of operation.

---

[15] Chainalysis, "OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses," (Aug. 10, 2023), https://www.chainalysis.com/blog/ofac-sanctions/.

[16] U.S. Department of the Treasury, "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," (Nov. 28, 2018), https://home.treasury.gov/news/press-releases/sm556.

[17] U.S. Department of the Treasury, "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex," (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701; U.S. Department of the Treasury, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange," (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471; U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," (Sep. 21, 2023), https://home.treasury.gov/news/press-releases/jy0364.

[18] U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916; U.S. Department of the Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768; U.S. Department of the Treasury, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," (Mar. 2, 2020), https://home.treasury.gov/news/press-releases/sm924.

[19] U.S. Department of Justice, "Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes," (Apr. 3, 2023), https://www.justice.gov/opa/pr/justice-department-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes#.