DEPARTMENT OF JUSTICE
JOURNAL OF FEDERAL LAW AND PRACTICE

Volume 69 May 2021 Number 3

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC 20530

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The Department of Justice Journal of Federal Law and Practice is published pursuant to 28 C.F.R. § 0.22(b).

The Department of Justice Journal of Federal Law and Practice is published by the Executive Office for United States Attorneys
Office of Legal Education
1620 Pendleton Street
Columbia, SC 29201

Cite as:
69 DOJ J. FED. L. & PRAC., no. 3, 2021.

Internet Address:
https://www.justice.gov/usao/resources/journal-of-federal-law-and-practice

Technology & Law

In This Issue

Introduction 1
Puneet V. Kakkar & Joseph Wheatley

Overcoming Technical Obfuscation: NITs and Remote Search Warrants 3
Puneet V. Kakkar & Joseph Wheatley

Introduction to the FinTech Ecosystem 23
Jill Westmoreland Rose, Kelli Andrews, & Karyn Kenny

Privilege in Data Breach Investigations 39
Brian Mund & Leonard Bailey

Using Blockchain Analysis From Investigation to Trial 59
C. Alden Pelker, Christopher B. Brown, & Richard M. Tucker

Prosecuting Sex Trafficking Cases in the Wake of the Backpage Takedown and the World of Cryptocurrency 101
Jane Khodarkovsky, April N. Russo, & Lauren E. Britsch

Finding Clarity in Crisis: How Technological Challenges Present Investigative Opportunities in the Time of a Pandemic 127
Denise O. Simpson & Nathaniel C. Kummerfeld

From Beepers to Smartphones: Challenges in Applying Title III to Modern Communication Technology 141
Jeffrey S. Pollak, Douglas D. Guidorizzi, & Shanai T. Watson

***Carpenter*'s Practical Implications for Law Enforcement and the Fourth Amendment** 159
Annamartine Salick & Anil J. Antony

Surfing the First Wave of Cryptocurrency Money Laundering 183
Alexandra D. Comolli & Michele R. Korver

Know Before You Go: Navigating Double Jeopardy Issues When Your Investigation Heads to Europe 237
Christen Gallagher

Crime in the Sky—Prosecuting Drone Offenses 255
Matthew J. Cronin

Technology & Law

In This Issue

DOJ and Drones: Protection, Policy, and Enforcement.....275
Colin T. Ross & Kevin M. Jinks

Recent Case Law Developments Involving the Crime–Fraud Exception: The Attorney–Client Privilege, Filter Teams Protocols, and Other Privileges.....289
Gretchen C. F. Shappert & Christopher J. Costantini

Note From the Editor-in-Chief.....355
Christian A. Fisanick

Using Blockchain Analysis From Investigation to Trial

C. Alden Pelker
Senior Counsel
Computer Crime & Intellectual Property Section

Christopher B. Brown
Assistant United States Attorney
District of Columbia

Richard M. Tucker
Senior Vice President, Legal, Privacy and Regulatory
CLEAR

Despite a growing and evolving legitimate user base, cryptocurrency—like cash—remains a popular means by which a wide range of criminal activities are funded and the proceeds of such activities are distributed. Cryptocurrency's decentralized, pseudo-anonymous nature, and the ease with which it can be moved across national borders with limited government oversight, make it attractive to cybercriminals, narcotics traffickers, and international organized crime groups, to name a few.

This article is meant to complement the recently published Department of Justice (Department) *Cryptocurrency Enforcement Framework* and build on the highly useful article that appeared in the 2019 Cybercrime and Cyber Threats edition of this journal: *Attribution in Cryptocurrency Cases*.[1] In the past two years, we have seen continued proliferation in the use of cryptocurrency by criminals and, far more concerningly, significant evolution in the means by which criminals can foil law enforcement authorities' efforts to develop attribution based on blockchain analysis. At the same time, however, the blockchain analysis tools available to law enforcement—many provided by third-party vendors—have become increasingly powerful and effective. This article seeks to survey the state of blockchain analysis in federal criminal investigations and to explore approaches for leveraging that analysis, both in the initial stages of an investigation and, far more interestingly, at trial.

---

[1] Michele R. Korver, et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233.

The first section of this article provides the technical framework for how cryptocurrency works, how blockchains may be analyzed, and ways those analysis techniques can be foiled or otherwise complicated. The second section describes how blockchain analysis can be used at the start of an investigation or in search warrant affidavits and other criminal process to advance such an investigation. The third and final section discusses ways to admit blockchain evidence at trial, as well as important considerations when admitting such evidence, including approaches to satisfying discovery obligations.

I. Introduction and background

A. What is a blockchain?

First, some necessary vocabulary and background: `Cryptocurrency`, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange.[2] Cryptocurrency users have one or more `addresses`, somewhat similar to bank account numbers and consisting of long strings of numbers and letters that users can trivially generate. Those addresses, on their own, have no correlation to their owners' real-world identities. Each address is a representation of a `public key` and has a corresponding `private key` that controls the ability to spend funds associated with the address.[3]

Cryptocurrencies are generally based on a distributed transaction ledger system called a `blockchain`.[4] A blockchain comprises a series of blocks, each of which contains data regarding batches of valid transactions. Each block also contains a cryptographic hash of the prior block of the blockchain, linking the blocks together and forming a chain of transactional information going back to the beginning of the ledger.

With a Bitcoin transaction from *A* to *B*, for example, the blockchain entry for that transaction will include three particularly significant categories of information:

---

[2] *Id.* at 233.

[3] For a more detailed discussion of cryptocurrency fundamentals, see JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS (2015).

[4] For a more detailed discussion of blockchains and how blockchains serve as cryptocurrency transaction records, see Peter Van Valkenburg, *What's a Blockchain, Anyway?*, COIN CTR. (Apr. 25, 2017), https://www.coincenter.org/education/blockchain-101/whats-a-blockchain/.

- one or more `inputs`—that is, the source (or sources) of the bitcoin being transferred in the transaction from *A* to *B*;
- an `amount`—that is, how much *A* transfered to *B*; and
- one or more `outputs`—that is, *B*'s Bitcoin address, or where the bitcoin should be transferred.

To initiate such a transaction using funds from her address, *A* (the payer) must cryptographically sign the transaction with her address' private key, which was generated when that address was created. Only the holder of a private key for a Bitcoin address can spend bitcoin from the address. A Bitcoin user can also spend from multiple Bitcoin addresses in a single transaction.

When a user creates a new transaction, she broadcasts that transaction to all the nodes in the network. Certain members of the network (often called `miners`) validate the transaction and include it in a proposed block. Eventually, the block containing that transaction (along with others) is added to the chain. On the Bitcoin blockchain, a new block is created every ten minutes, on average, and with each block, an average of approximately 2,000 new transactions are added to the blockchain.[5] The blockchain is constantly updated and stored by full nodes—members of the Bitcoin network, including many miners, who store and share full copies of the blockchain.

The transactional information contained in the blockchain does not explicitly identify the parties to any given transaction. By analyzing the blockchain, however, it is possible, in some cases, to identify (or make a reasonable inference about) the owner of a particular Bitcoin address.

B. Blockchain analysis techniques

Because details of every transaction are stored within the blockchain, the most conceptually intuitive type of blockchain analysis involves reviewing the transaction history and following the movement of funds over time from one address to another—a process

[5] For a more detailed discussion on mining, see Peter Van Valkenburg, *What is Bitcoin Mining, and Why is it Necessary?*, COIN CTR. (Dec. 5, 2014), https://www.coincenter.org/education/advanced-topics/mining/.

sometimes called tracing.[6] With Bitcoin, for example, anyone can see any Bitcoin transaction since the inception of that cryptocurrency, either by downloading a copy of the blockchain through the network itself or by using a publicly available blockchain explorer, such as the one available at blockchain.com/explorer. Attempted manually, such tracing is cumbersome and time consuming, but a growing collection of new technology companies offer tools to make this analysis faster and more efficient.

Of course, tracing the movement of funds along the blockchain does not necessarily identify a specific address owner or party to a particular transaction. But the owners of some addresses can be identified through a number of ways off-chain—that is, based on information obtained from a source other than the blockchain itself. For example, users sometimes post their Bitcoin wallets on social media and forums. Labeling an address with a real-world identity is sometimes called tagging. And where tracing analysis leads through one or more tagged addresses, making highly probable inferences about a transaction's participants becomes increasingly possible.

Another blockchain analysis technique is identifying linked addresses (or clusters) held by an individual or organization. One common protocol for cluster analysis is linking together all the input addresses for one transaction. That is, if two or more addresses are inputs of the same transaction with one output, then one can infer that those input addresses are controlled by the same user. This common input or co-spend analysis is highly reliable and is the most-used metric in commercial blockchain analysis tools. Another clustering heuristic is to identify a transaction's change address, which is the sender's address that receives any remainders of transferred funds from a transaction that spends a smaller amount of virtual currency than the amount associated with the sender's input(s). If such a change address is identified, then the ultimate output of that address and all the original inputs of the transaction may be controlled by the same user. While clustering can be done manually, doing so would be cumbersome and limited; instead, law

[6] This is true for Bitcoin and other cryptocurrencies with public blockchains. Other "anonymity enhanced cryptocurrencies" use non-public blockchains, making it much more difficult to trace funds.

enforcement uses commercially available blockchain analysis tools to streamline the process.[7]

Law enforcement and regulators use a wide range of blockchain analysis tools to apply these analysis techniques, many of which are provided by third-party companies like Chainalysis, TRM Labs, and Elliptic. There are also free basic blockchain analysis tools that allow users to view the transaction history associated with a given address. While those free tools may allow the user to perform some basic tracing, they, unfortunately, are often incapable of employing clustering or other more involved techniques for tracing or attributing more complex cryptocurrency transaction histories.

C. Obfuscating the transaction history on the blockchain

Clustering, off-chain data scraping, tracing, and other blockchain analysis techniques can be foiled by a variety of cryptocurrency money laundering techniques popular with even relatively unsophisticated criminals. For example, third-party crypto `mixing`—or `tumbling`—services shuffle a user's bitcoins with other users' cryptocurrency to release a fresh batch of bitcoins from a random address. The process, which users typically pay a variable fee for, breaks the transaction trail and usually makes tracing highly impractical.

Another obfuscation technique is known as `chain hopping`, moving assets from one cryptocurrency to another, often through a rapid succession of transactions. Paid chain-hopping services specialize in executing these transfers in a manner that may make them very difficult for investigators to detect and analyze. This difficulty is exacerbated when the chain hopping involves anonymity enhanced cryptocurrencies with non-public blockchains.

`Peel chains` are another means by which users obfuscate blockchain transaction histories. A peel chain occurs when a large amount of bitcoin sitting at one address is sent through a series of transactions in which a slightly smaller amount of bitcoin is transferred to a new address with each transaction. In each of these steps, some quantity of bitcoin "peels off" the chain to another

---

[7] *See, e.g.,* United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020) (stating that no Fourth Amendment privacy interest existed where agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by the targets).

address—frequently to be deposited into a virtual currency exchange—and the remaining balance is transferred to the next address in the chain. This technique is growing in popularity: Peel chains were employed by North Korea-based cybercriminals targeted in a recent case out of the District of Columbia.[8]

II. Blockchain analysis in investigations

Many criminal cases begin and end successfully when investigators remember the wise adage, "follow the money." This strategy holds with cryptocurrency, and investigators increasingly rely on blockchain analysis to both identify criminal actors and build a case against them. As you consider whether and how to incorporate blockchain analysis into your investigative strategy, be forewarned: There may be myriad challenges—legal and practical—to admitting blockchain analysis evidence at trial. For example, some analytical tools may incorporate sensitive or proprietary techniques that cannot be readily presented in open court. As discussed further below, these difficulties are hardly insurmountable, but a savvy prosecutor may conclude that employing tools in other ways that avoid undue litigation risk may be the more prudent course.

Given these challenges, consider from the outset what role blockchain analysis should play the investigation. Of course, the answer may be dictated by simple necessity, such as where there is no other viable avenue for developing attribution evidence.

A. Tips and leads for identifying investigative targets

Many successful investigations begin with a tip from a confidential source. The admissibility—even the veracity—of such "tips and leads" are rarely, if ever, the subject of litigation.[9] Likewise, blockchain analysis can be a useful tool simply for identifying investigatory targets of merit.

---

[8] Complaint, United States v. 113 Virtual Currency Accounts, No. 20-cv-606 (D.D.C. Mar. 3, 2020), ECF No. 1.

[9] A grand jury needs no probable cause to initiate an investigation. The impetus for the investigation may be "tips, rumors, evidence proffered by the prosecutor, or the personal knowledge of the grand jurors." Branzburg v. Hayes, 408 U.S. 665, 701 (1972).

Investigators can identify addresses of interest through online undercover operations or publicly posted addresses on criminal forums, or through a transaction analysis to flag large payments or especially active addresses. And once a subject address is identified, a tracing analysis can provide investigators with a sense of scope—that is, how much money has moved into and out of a particular wallet associated with a darknet child pornography marketplace or known jihadist forum over a longer period of time?

In addition to these techniques for proactively identifying addresses that may be engaged in illicit activities, investigators may also receive valuable leads from cryptocurrency exchanges, which are considered money services businesses (MSBs) and, thus, are obligated to have anti-money laundering programs and file suspicious activity reports (SARs) and other notifications under the Bank Secrecy Act. Subpoenas to cryptocurrency exchanges may even allow investigators to obtain valuable attribution evidence as to the owner of a particular address.[10]

Once a target is identified based on suspicious cryptocurrency transactions, a SAR from an exchange, or other such methods, investigators may conclude that further blockchain analysis is not necessary or worthwhile, electing instead to pursue more traditional investigative techniques—ranging from real-world surveillance to social media search warrants—to build a case against the individual. By treating suspicious cryptocurrency transactions and any associated blockchain analysis as tips and leads only, investigators will forego the use of evidence from blockchain analysis in their case-in-chief, but they will also avoid the evidentiary and logistical challenges associated with using of such evidence at trial.

B. Use in criminal process

In addition to using blockchain analysis for pure lead purposes, it can also be used in search and seizure warrants. Similar to instances where blockchain analysis leads to a subpoena or a Financial Crimes Enforcement Network database query at the initiation of an investigation, its use in warrants is often an intermediate step used to justify searching a subject's residence, digital devices, or other

[10] This is true with centralized exchanges that are responsive to legal process. Peer-to-peer transactions conducted via decentralized exchanges (DEXs) may foil such efforts at attribution, however.

location—with the understanding that the fruits of that search (such as drug paraphernalia, child pornography, incriminating text messages, etc.) will provide the primary evidence of the subject's guilt at trial, rather than the blockchain analysis.

That raises the question of how courts should weigh blockchain analysis in evaluating probable cause for a search or seizure. As the Supreme Court has stated, probable cause requires only a "'fair probability' on which 'reasonable and prudent [people,] not legal technicians, act.'"[11] "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules."[12] Under this "totality-of-the-circumstances approach," there is no one-size-fits-all approach to using blockchain analysis in warrant applications.[13]

1. Lessons from the law of anonymous tips

A starting point for analysis might be how courts assess information from informants or anonymous tipsters. One representative formulation by the Seventh Circuit holds that probable cause depends on the informant's "reliability, veracity and basis of knowledge."[14] Of these factors, reliability is probably the most important to address for blockchain analysis. Few questions should arise about the basis of knowledge or veracity. The basis of knowledge for blockchain analysis—that is, the source of information used to conduct such analysis—is, generally speaking, the blockchain itself.[15] The blockchain is an open-source, publicly available database relied upon by users around the world for up to hundreds of thousands of

---

[11] Florida v. Harris, 568 U.S. 237, 244 (2013) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)) (alteration in original).
[12] *Gates*, 462 U.S. at 232.
[13] *Id.* at 230.
[14] United States v. Orr, 969 F.3d 732, 736 (7th Cir. 2020) (quoting United States v. Olson, 408 F.3d 366, 370 (7th Cir. 2005)); *see also Gates*, 462 U.S. at 230 (stating that veracity, reliability, and basis of knowledge "should be understood simply as closely intertwined issues that may usefully illuminate the common-sense, practical question whether there is 'probable cause' to believe that contraband or evidence is located in a particular place").
[15] More sophisticated applications of blockchain analysis may draw on other sources of information for attribution or more accurate clustering.

transactions per day.[16] There is no serious question that the blockchain accurately captures the transactional data used in blockchain analysis. In a similar vein, the blockchain is the product of an automated process (for example, the Bitcoin protocol), so it makes little sense for a court to question the veracity of the data the way it might inquire into the motives or trustworthiness of an informant.

Reliability is a more complicated question: Can you reliably use blockchain analysis to trace funds from one wallet address to another? At its most basic level, blockchain analysis is not that much different than tracing funds from one bank account to another. If attribution is not at issue—for example, in a seizure warrant intended to recover the proceeds of a fraud or hack—it may be enough for the warrant to list out the "audit trail" of hops from the originating address to the final resting point. In a sense, this is not really blockchain "analysis" at all; it is simply using the blockchain as a source of transactional information, just as an affidavit might rely on bank records to show the transfer of funds from a victim's bank account, through intermediary accounts, to the account targeted for seizure.

In other cases, blockchain analysis might be used to explain audit trails that are too long or too complicated to be narrated in detail, or to show attribution and ownership through a series of transactions (such as a peel chain). Here, it may be appropriate for the affidavit to address the reliability of blockchain analysis as used to support probable cause. There are several possible approaches.

First, the affidavit could identify the underlying assumptions and logic used in grouping clusters—such as co-spending or change addresses—and explain that the assumptions are based on commonly observed patterns of transactional behavior. Second, the affidavit could note the generally reliable track record of blockchain analysis in other contexts.[17] This might include similar investigations conducted by law enforcement. It might also include the growing use of blockchain analysis in the private sector as a due diligence and anti-money laundering (AML) tool. Third, the affidavit could cite other

---

[16] *See Bitcoin*, COINDESK, https://www.coindesk.com/price/bitcoin (last visited Feb. 11, 2021) (showing 340,736 transactions valued at $12.45 billion during preceding 24-hour period).

[17] *See* United States v. Bradley, 924 F.3d 476, 480 (8th Cir. 2019) ("An 'informant's track record of providing trustworthy information' establishes reliability.") (quoting United States v. Faulkner, 826 F.3d 1139, 1144 (8th Cir. 2016)).

corroborating evidence generated in the investigation.[18] For example, in a drug trafficking investigation, blockchain analysis might be used to identify a subject cashing out cryptocurrency proceeds derived from a darknet vendor—perhaps through a long, complicated chain of transactions that eventually winds up at an identifiable exchange account. Here, blockchain analysis serves two functions: It traces the transactions, and it attributes them to a single actor engaged in multiple laundering transactions (as opposed to multiple independent actors engaged in one-off commercial transactions). Thus, to the extent there is other, more traditional evidence linking the subject to drug trafficking activity, that evidence serves to corroborate the critical attribution element of the blockchain analysis.

2. Comparison to software used in child pornography investigations

To our knowledge, there are no published decisions analyzing the weight or reliability of blockchain evidence in a search warrant application.[19] But—with important caveats—some lessons might be

---

[18] *See* United States v Colkley, 899 F.2d 297, 302 (4th Cir. 1990) (reasoning that an anonymous tip "was sufficiently detailed and sufficiently corroborated by independent police work to come within the standards of probable cause articulated in *Gates*").

[19] On January 6, 2021, a magistrate judge in the District of Columbia issued a Rule 41 premises search warrant for the home of a subject suspected of using bitcoin to purchase child pornography from an Tor-based child pornography website, authorizing, *inter alia*, the seizure of cryptocurrency found at the premises used to commit and promote the child pornography offenses. *See In re* Search of One Address in Washington, D.C. Under Rule 41, No. 20-sw-314, 2021 WL 49928 (D.D.C. Jan. 6, 2021) [hereinafter *Search of One Address*]. In a written opinion accompanying the warrant, the court noted that blockchain analysis was responsible for identifying the cryptocurrency exchange used by the illegal website, and that records from the cryptocurrency exchange in turn revealed the identity of the subject. *Id.* at *2 ("Blockchain analysis revealed that Website 1 used a 'payment processing service . . . operated by a known cryptocurrency exchange service (the "Exchange") located in the United States' to effectuate the illicit transactions. By subpoenaing the Exchange, law enforcement obtained documents revealing the identity of the Subject.") (quoting warrant affidavit) (internal citations omitted). The court did not, however, expound on how much weight it placed on the blockchain analysis in the overall determination of probable cause to search the subject premises.

drawn from the growing body of case law affirming the use of automated software tools in child pornography investigations to identify users sharing child exploitation material online. For example, in *United States v. Thomas*, the Second Circuit considered a warrant based primarily on a proprietary software suite known as Child Protection System (CPS).[20] As the Second Circuit explained, CPS simply automates the process of a law enforcement officer manually querying peer-to-peer (P2P) file sharing networks for known child exploitation material: "CPS automates this process by canvassing these public P2P networks, identifying files that contain child pornography, cataloguing this information, and providing law enforcement officers with a list of the online users who are sharing these files over P2P networks."[21] In *Thomas*, CPS was used to identify a suspect Internet Protocol (IP) address, which agents then used to identify a physical address, conduct surveillance, and obtain a search warrant. The Second Circuit held that the CPS software established sufficient probable cause to link the illicit activity to the target premises, emphasizing the fact that the software merely automated a process that could otherwise be done manually.[22] That was sufficient to distinguish the use of CPS software from drug-sniffing dogs, the proper employment of which requires "numerous steps, each of which is susceptible to error."[23] The Sixth Circuit followed suit in *United States v. Dunning*, relying in part on *Thomas* to affirm the sufficiency of an affidavit based on CPS.[24] In addition, the Sixth Circuit cited the affiant's training and experience with the software, noting that he "was trained to use, and had previously used, software to investigate child pornography crimes."[25]

Like the software tools described above, blockchain analysis software largely serves an aggregation function. In theory, most analysis of blockchain transactions could be done by hand. But in cases involving hundreds, or perhaps thousands, of transactions—given the ability of criminals to generate limitless new addresses and to use software tools to create automated spending algorithms—much of the functionality provided by blockchain analysis software lies in its

---

[20] 788 F.3d 345, 348 (2d Cir. 2015).
[21] *Id.*
[22] *See id.* at 352.
[23] *Id.*
[24] 857 F.3d 342, 347–48 (6th Cir. 2017).
[25] *Id.* at 347.

ability to pull massive amounts of transactional data from the blockchain and provide user-friendly tools to explore it.[26] To be sure, there are limits to this analogy. Blockchain analysis software does not *only* aggregate blockchain data; it also applies heuristics and other analytical tools to cluster addresses into related groups. But not every warrant needs to rely on those additional functions. To the extent blockchain analysis software is used simply to "follow the money" in a warrant affidavit, cases like *Thomas* and *Dunning* should lend support.

This line of cases has yielded a few additional points that are relevant to using proprietary blockchain analysis software platforms to support probable cause in an affidavit. First, neither the identity of the specific company nor the underlying software code is important to the probable cause analysis. As the Second Circuit explained in *Thomas*, "the primary relevance of automating third-party software lies not in its name, but in its *functionality*," and it was sufficient where "the affidavit disclosed that law enforcement used automated software during the course of this investigation, noted the software's purpose, and then went into considerable detail as to how the software operated."[27] Second, the software's conclusions need not rise to the level of scientific certainty to establish probable cause.[28] And third, courts have carefully distinguished between the use of software tools to establish probable cause in a warrant from their admissibility at

---

[26] *See, e.g.*, *Search of One Address*, 2021 WL 49928, at *2 (noting that "law enforcement can use publicly-available software to analyze the BTC blockchain by 'forensically examining, tracing, and mapping data on the blockchain . . . to unmask the identities of specific users of a given cryptocurrency wallet'") (quoting search warrant affidavit).

[27] *Thomas*, 788 F.3d at 351; *cf. Dunning*, 857 F.3d at 346–47 (rejecting defense argument that affidavit could not rely on CPS without explaining software's "source code").

[28] *See, e.g.*, United States v. Chiaradio, 684 F.3d 265, 279 (1st Cir. 2012) (rejecting defense challenge to scientific reliability of EP2P software "[b]ecause probable cause 'does not require scientific certainty'") (quoting Roche v. John Hancock Mut. Life Ins. Co., 81 F.3d 249, 254 (1st Cir. 1996)); United States v. Schumacher, 611 F. App'x 337, 340 (6th Cir. 2015) (not precedential) (rejecting defense challenge based on "scientific reliability" of software).

trial.[29] This is a particularly important point for blockchain analysis: Probable cause and admissibility are different questions, governed by different standards and separate bodies of law. Prosecutors should resist efforts by courts or defense counsel to view warrant applications through the lens of technical evidentiary rules.

C. Blockchain analysis in civil forfeiture complaints

Finally, two recent civil forfeiture actions involving cryptocurrency thefts linked to North Korea provide public examples of blockchain analysis in action.[30] It should be noted that civil forfeiture complaints are not the same as warrant affidavits. They are subject to a lower standard of proof than search warrants.[31] At the same time, they are public pleadings used to announce the government's case—roughly equivalent to an indictment or criminal complaint—and may include more detail than strictly necessary to meet the relevant legal threshold. In any event, these complaints offer rare public examples, readily adaptable to warrant affidavits, of how blockchain evidence can be described and relied upon.

The complaints include a succinct introduction to blockchain analysis in their background sections. For example:

> While the identity of a BTC/ETH address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can identify the owner of a particular BTC/ETH address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many BTC addresses to receive payments from different customers. When the user wants to transact the BTC that it has received (for example, to exchange BTC for

---

[29] *See, e.g.*, *Chiaradio*, 684 F.3d at 279 (rejecting defense argument that software was "too untested to meet the requirements of the Federal Rules of Evidence" because "[t]his argument mixes plums and pomegranates; the Federal Rules of Evidence do not apply" to the probable cause standard).
[30] Complaint, *supra* note 8; Complaint, United States v. 280 Virtual Currency Accts., No. 20-CV-02396 (D.D.C. Aug. 27, 2020), ECF No. 1 [hereinafter Complaint, *280 Virtual Currency Accts.*].
[31] *See* United States v. Mondragon, 313 F.3d 862, 864–66 (4th Cir. 2002) (reasonable belief).

> other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying the virtual currency transactions.[32]

A similar summary of blockchain analysis could be included in warrant affidavits, especially in cases where blockchain analysis is used in more sophisticated ways to cluster and attribute addresses.[33]

The complaints also cite or refer to blockchain analysis when discussing specific transactions. For example, in discussing a publicly reported hack of a cryptocurrency exchange, the complaint in *280 Virtual Currency Accounts* explains that "[b]lockchain analysis corroborated [the exchange's] statements and provided more detail for the following thefts/transactions."[34] In another example, blockchain analysis was used to trace funds through a series of clusters; the complaint explains that the pattern "illustrat[es] common ownership as the funds regroup at the same destination after being layered."[35] Nevertheless, not every element of the narrative relies on the analytical functions of blockchain analysis—at multiple points, the complaints simply list out individual transactions or include charts showing the step-by-step movement of funds. The same approach could be taken in a warrant affidavit.

III. Blockchain analysis at trial

In recent years, virtual currency use has dramatically expanded, as has criminal investigation and prosecution of crimes involving virtual

---

[32] Complaint, *280 Virtual Currency Accts.*, *supra* note 30, at ¶ 13.
[33] A concise overview of blockchain tracing methodology also appears in *Search of One Address*, 2021 WL 49928, at *2.
[34] Complaint, *280 Virtual Currency Accts.*, *supra* note 30, at ¶ 27.
[35] *Id.* ¶ 44.

currency.[36] Despite the broad use of blockchain analysis in a variety of cases, see Section II., *supra*, litigation regarding its admissibility has been limited.[37] Some legal writers—albeit mostly law students—have even questioned its admissibility entirely.[38] Luckily, examining the Federal Rules of Evidence reveals multiple clear paths to the admission of blockchain evidence.[39] This section discusses methods for authenticating blockchain evidence, clarifies why the blockchain should not be excluded as hearsay and does not present a Confrontation Clause problem, and addresses trial strategies for

---

[36] *See generally* U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASKFORCE: CRYPTOCURRENCY ENFORCEMENT FRAMEWORK (Oct. 2020).

[37] The earliest instance of blockchain evidence being admitted in a significant federal trial appears to be the Silk Road trial in 2015. There, the government used screenshots from Blockchain.info to depict the Bitcoin transactions related to the Silk Road Marketplace. Transcript at 1729–32., United States v. Ulbricht, 14-cr-68 (S.D.N.Y Jan. 29, 2015), ECF No. 212. This approach was similarly taken by the government in *United States v. Michael Brown* the following year. Transcript, *United States v. Brown,* No. 3:13-cr-118 1, 98 (M.D. Tenn. May 10, 2016) (Where the Blockchain.info records were particularly relevant because the defendant visited the Blockchain.info page for the bitcoin address at issue). Bitcoin and/or blockchain-related evidence has also been admitted in, *inter alia*, *United States v. Costanzo,* 956 F.3d 1088 (9th Cir. 2020) and *United States v. Ologeanu*, No. 18-cr-81, 2020 WL 1676802, at *10–*11 (E.D. Ky. Apr. 4, 2020).

[38] *See, e.g.*, Angela Guo, *Blockchain Receipts: Patentability and Admissibility in Court*, 16 CHI.-KENT J. INTELL. PROP. 440, 444–45 (Apr. 2017) ("[T]he admissibility of these distributed ledger receipts has not been entirely settled."), J. Collin Spring, *The Blockchain Paradox: Almost Always Reliable, Almost Never Admissible*, 72 SMU L. REV. 925, 935 (2019) ("blockchain evidence is almost always inadmissible in federal court, and is only admissible under limited, factually specific scenarios."). *But see* George Bellas, *Blockchain as Evidence*, 66 ILL. STATE BAR ASS'N–TRIAL BRIEFS NO. 3 (Nov. 2019) (observing that introducing blockchain data as evidence at trial "[s]ounds daunting, but it is really not that complicated," while discussing the applicability of Illinois state rules of evidence that parallel the federal rules).

[39] To avoid any issue, Vermont went so far as to enact legislation specifically declaring blockchain evidence self-authenticating. H.868 (Act 157) (Vt. 2016) ("A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902.").

admitting blockchain evidence and related testimony before concluding with a brief discussion of discovery considerations.

A. Authentication

As explained in Section I., *supra*, a blockchain is an immutable ledger that serves as a tamper-proof record of all confirmed transactions.[40] The blockchain serves as the ground truth for cryptocurrency transactions—if a transaction is recorded on a blockchain, the transaction definitively occurred, because its presence on the blockchain is what defines the transaction's occurrence.[41] Metaphysics aside, the blockchain is inherently well-positioned to address the core goal of the authentication requirements of the Federal Rules of Evidence—to show that proffered evidence is what the proponent claims it to be.[42]

Rule 901 sets forth a non-exhaustive list of common methods for authenticating evidence. The applicability of several of the methods to blockchain evidence is addressed below. Prosecutors should be mindful that the methods enumerated in Rule 901 are illustrative, not comprehensive. Indeed, when considering authentication of electronic evidence, at least some courts "have been willing to think 'outside of the box' to recognize new ways of authentication."[43]

1. Witness with knowledge

One of the easiest ways to authenticate the blockchain is perhaps the most easily overlooked—through the testimony of a foundation witness.[44] For most virtual currencies, the blockchain is publicly available and can be downloaded directly by any member of the network.[45] The Bitcoin blockchain file is over 300 GB and growing

---

[40] *See Gratkowski*, 964 F.3d at 309 n.2 (defining blockchain as "a technological advancement that permits members in a shared network to 'record a history of transactions on an immutable ledger.'").

[41] *See Costanzo*, 956 F.3d at 1093 ("Each transaction was complete only after it was verified on the blockchain.").

[42] FED. R. EVID. 901.

[43] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 552 (D. Md. 2007).

[44] FED. R. EVID. 901(b)(1).

[45] For the purposes of this article, we have focused on publicly available blockchains. Presenting evidence regarding transactions conducted through anonymity-enhanced cryptocurrencies (AECs) may necessitate different considerations.

constantly with each new block that is confirmed.[46] A government witness versed in virtual currency could easily download a copy of the blockchain and explain it conceptually to the jury. Such testimony would also readily fit within Rule 901(b)(9), evidence about a process or system,[47] and could be bolstered by a discussion of the distinctive characteristics of the blockchain pursuant to Rule 901(b)(4),[48] all of which would aid in authenticating the evidence.

2. Rule 902 certifications

While prosecutors offering blockchain evidence will almost certainly want to offer testimony to put it into context, see Section III.C., *infra*, there are several options for admitting blockchain evidence as self-authenticating under Rule 902. This may help avoid the unnecessary hassle of calling a witness purely for authentication purposes.[49]

In many cases, blockchain records may be admitted as business records under Rule 902(11).[50] This rule allows a record that meets the requirements of Rule 803(6) to be admitted with a certification from the records custodian.[51] Rule 803(6), discussed further in Section III.B., *infra*, pertains to a record of, *inter alia,* an act, event, or condition where the record was "made at or near the time by—or from information transmitted by—someone with knowledge" and "kept in the course of a regularly conducted activity of a business, organization, occupation, or calling," where "making the record was a

---

[46] *Blockchain Size (MB)*, BLOCKCHAIN.COM, https://www.blockchain.com/charts/blocks-size (last visited Feb. 11, 2021.).

[47] FED. R. EVID. 901(b)(9).

[48] FED R. EVID. 901(b)(4).

[49] *Contra* Michael L. Levy & John M. Haried, *Practical Considerations When Using New Evidence Rule 902(13) to Self-Authenticate Electronically Generated Evidence in Criminal Cases*, 67 DOJ J. FED. L. & PRAC. no. 1, 2019, at 84 ("With unfamiliar technology, it is certainly conceivable that some judges will not be satisfied with anything less than a live witness explaining the process.").

[50] Guo, *supra* note 38, at 448. ("The blockchain receipts and the consensus algorithm are quintessential examples of record-keeping in the ordinary course of business.").

[51] FED R. EVID. 902(11).

regular practice of the activity."[52] Courts have confirmed that "computer data compilations" may be business records.[53]

The blockchain is a living record, with new blocks of transactions being appended with each confirmation at roughly 10-minute intervals. This easily satisfies the temporal element of the first requirement, that the record be made at or near the time of the transaction. The record is made by the miner validating the transaction block, based on the information relayed to it by the computers announcing the proposed transactions. (Alternatively, if a court determines that the virtual currency transactions are hearsay-eligible statements of the sender rather than computer-generated records, the "someone with knowledge" would be the sender himself, who transmitted the information to the other members of the virtual currency network upon signing and announcing the transaction.) The blockchain is necessarily kept in the course of miners' and node operators' regularly conducted activity, and making the record is a regular practice of their activity—indeed, the maintenance of the blockchain is the core function of these virtual currency participants. It bears emphasizing that this analysis is not limited to miners but applies to many parties that operate nodes and keep and maintain a copy of the blockchain as part of their regularly conducted activity.

Prosecutors may have multiple options in determining who should certify the blockchain records. Rule 902(11) allows the certification to be completed by "the custodian or *another qualified person*."[54] As the advisory committee notes to Rule 803(6) comment, there is no requirement that the witness be involved as a participant in the matters reported.[55] Rather, the records may be admitted through someone acting merely as an observer.[56] Indeed, courts have long held that the other "qualified witness" only need to understand the record

---

[52] FED R. EVID. 803(6).

[53] Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980); United States v. Fendley, 522 F.2d 181 (5th Cir. 1975).

[54] FED. R. EVID. 902(11) (emphasis added).

[55] FED. R. EVID. 803(6) advisory committee's note to 1972 proposed rules ("Occasional decisions have reached for enhanced accuracy by requiring involvement as a participant in matters reported. . . . The rule includes no requirement of this nature. Wholly acceptable records may involve matters merely observed . . .").

[56] *Id.*

keeping system to authenticate the evidence.[57] This is significant in the blockchain context: It confirms that one need not be a miner or the operator of a full node involved in relaying and verifying transactions to appropriately certify the blockchain. Rather, any individual who directly obtains a copy of the blockchain and meets the remaining requirements under 803(6) may provide a certification under 902(11). This may extend to virtual currency exchanges, wallet hosting providers, law enforcement blockchain specialists, academics, and even blockchain enthusiasts. An analyst specializing in blockchain analysis who regularly maintains a copy of the blockchain to perform her blockchain analysis duties in her organization would easily meet the requirements for providing a certification under 902(11).

Blockchain evidence may also be authenticated using a certification issued pursuant to Rule 902(13). Under Rule 902(13), certified records generated by an electronic process or system that produces accurate results are self-authenticating.[58] Rule 902(13) was adopted in December 2017 and sought to make it easier for parties to authenticate certain types of electronic evidence without "the expense and inconvenience of producing a witness" unnecessarily.[59]

The core code underlying Bitcoin and most decentralized virtual currencies[60] is designed to ensure that the blockchain is resistant to any attempted manipulation. The entire transaction verification and validation process is intended to further bolster the sanctity of the

---

[57] United States v. Salgado, 250 F.3d 438, 452–53 (6th Cir. 2001) (the authenticating witness must merely be "familiar with the record keeping system employed" but need not have programmed the computer herself or be an expert on the details of the computer processes pursuant to which the records are created, maintained, and produced). Levy & Haried, *supra* note 49, at 86 (citing United States v. Ray, 930 F.2d 1368, 1369–70 (9th Cir. 1990); United States v. Franco, 874 F.2d 1136, 1139–40 (7th Cir. 1989); United States v. Hathaway, 798 F.2d 902, 905–07 (6th Cir. 1986)).

[58] FED. R. EVID. 902(13).

[59] FED. R. EVID. 902(13) advisory committee's note to 2007 amendment.

[60] Prosecutors dealing with non-mainstream virtual currencies with smaller user bases that may have adapted their code in a way that introduced security vulnerabilities or allow for transaction manipulation (inadvertently or intentionally) will need to provide additional facts to show that the blockchain records for that particular virtual currency were the product of a process or system that produces an accurate result. Even given the thousands of virtual currencies currently in existence, this is likely to be a real consideration in only a very small number of cases.

data contained in the blockchain. As explained in Section I., *supra*, virtual currency transactions are signed by the sender's private key, validated by nodes, confirmed by miners, and then added to the blockchain, whereupon subsequent node operators and miners affirm the integrity of the transaction by accepting the block in which the transaction is contained and adding new blocks on top of it. In short, the blockchain has extensive built-in protections to ensure the system or process produces an accurate result.

The addition of Rule 902(13), along with Rule 902(14)—which deals with authenticating forensic images and was adopted at the same time—was accompanied by several noteworthy pieces of legal scholarship discussing the applicability of the rules.[61] Much of the discussion incorporated scenarios developed by John Haried, Criminal eDiscovery Coordinator at the Department, who originally proposed the amendments at the advisory committee's symposium on electronic evidence.[62] In collaboration with the reporter to the Evidence Rules Committee, Haried developed several hypotheticals articulating the applicability of the new rules to particular fact patterns. These scenarios and the related analysis were incorporated into a treatise on authenticating digital evidence co-authored by the reporter to the Judicial Conference Advisory Committee on Evidence Rules and former members of Judicial Conference advisory committees, including the Honorable Paul Grimm, widely regarded as an expert in electronic evidence matters.[63] In general, the applicability of the rules to the stated scenarios carries far more persuasive and authoritative weight than would otherwise be warranted for analysis contained in a typical law review article.

A review of these scenarios provides useful corollaries to admitting blockchain evidence. In one, the proponent uses Rule 902(13) to authenticate a web server log that automatically records certain information about every computer that views a website and captured the hacker-defendant's IP address.[64] In another, the proponent uses

---

[61] John M. Haried, *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*, 66 U.S. ATTY'S BULL., no. 1, 2018, at 127; Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. *1 (2017); Levy & Haried, *supra* note 49, at 81.

[62] *See* Grimm, *supra* note 61, at *42 n.138; Symposium, *The Challenges of Electronic Evidence*, 83 FORDHAM L. REV. 1163, 1192–97 (2014).

[63] Grimm, *supra* note 61, at *42 n.138.

[64] *Id*. at *43–*44.

Rule 902(13) to authenticate records from the Windows registry indicating that a particular USB drive was plugged into a particular computer:

> With Rule 902(13), the proponent of the evidence could obtain a written certification from the forensic technician, stating that the Windows operating system regularly records information in the Windows registry about USB devices connected to a computer; that the process by which such information is recorded produces an accurate result; and that the printout accurately reflected information stored in the Windows registry of [the defendant's] computer.[65]

The blockchain is much like the web server log or Windows registry log discussed in the hypotheticals above, except it records and stores records of virtual currency transactions, rather than records of IP address access to a server or USB drive connections to a computer. The blockchain also produces an accurate result, recording the virtual currency transactions in their true form. The additional verification and validation protections built into the blockchain ensure a result even more accurate than that contemplated by a web server log or Windows registry log.[66]

To satisfy Rule 902(13), the certification may need to provide additional background regarding the blockchain to establish the reliability of the system or process.[67] As the advisory committee notes explain, the certification must provide information that would be sufficient to authenticate the record if the certifying person testified.[68]

---

[65] *Id.*

[66] *See generally* United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) (Once authenticated, questions about the accuracy of computer-generated records resulting from incorrect data entry or the operation of the computer program affect "only the weight of the printouts, not their admissibility.").

[67] *See generally* Levy & Haried, *supra* note 49 (Observing that "[m]achine-generated records from less familiar systems and processes . . . may require a more factually detailed certification," and noting that a more detailed certification may be required "if the defense contests [an] issue, or you have a cantankerous technophobe for a judge.").

[68] FED R. EVID. 902(13) advisory committee's note to 2017 amendment.

For a technology such as blockchain, which may be unfamiliar to the judge, more detail may be needed.[69]

Prosecutors may consider drafting a hybrid certification meeting the requirements of Rule 902(11) and Rule 902(13), similar to the hybrid 902 certifications commonly used to authenticate records obtained from electronic communication services. Proponents of the evidence should also be mindful that certifications under Rule 902(11) or Rule 902(13) change the *manner* in which evidence can be authenticated, but not the *standards* for authentication; if the testimony of the certifying witness would be insufficient to authenticate the records, the defect is not cured by presenting a certification rather than live testimony.[70] While proper certifications should not present Confrontation Clause issues, the matter is discussed in Section III.C., *infra*.

3. Judicial notice

A court may also take judicial notice of the blockchain pursuant to Rule 201. Courts have broad discretion to take judicial notice of evidence that, like the blockchain, can be "accurately and readily determined from sources whose accuracy cannot reasonably be questioned."[71] Courts have taken judicial notice of facts produced by an electronic process, including, notably, GPS data,[72] Google Maps,[73]

---

[69] Levy & Haried, *supra* note 49, at 84 ("The more familiar the technology is to the judge (and jury), the more likely a simple certification will suffice.").
[70] Grimm, *supra* note 61, at *1 ("These new amendments do not change the *standards* for authentication of electronic evidence. Rather, they change the *manner* in which the proponent's submission on authenticity can be made. Instead of calling a witness, the proponent can provide a certificate prepared by the witness of the submission that he would have made if required to testify. Of course, if that submission would be insufficient if he *had* testified, these new amendments will be of no use. An insufficient showing of authenticity does not somehow become better by way of a certificate in lieu of testimony.").
[71] FED R. EVID. 201.
[72] United States v. Brooks, 715 F.3d 1069 (8th Cir. 2013) (taking judicial notice of the accuracy and reliability of GPS technology in admitting GPS data obtained from a tracker placed in an envelope of stolen money in a bank robbery prosecution).
[73] *See, e.g.*, United States v. Burroughs, 810 F.3d 833, 835 n.1 (D.C. Cir. 2016) (Taking judicial notice of a Google Map, because, "It is a 'source[] whose accuracy cannot reasonably be questioned,' at least for the purpose of

and time and date information.[74] One court, finding the record deficient, even conducted its own research and took judicial notice that a "tack" marking coordinates on a Google Map was automatically generated, not manually placed and labeled.[75]

In requesting a court take judicial notice of blockchain records, a party should be prepared to provide the court with sufficient information to determine that the blockchain source's "accuracy cannot reasonably be questioned."[76] The background information on the blockchain in Section I., *supra*, and the references to the blockchain as the ground truth of virtual currency transactions in Section III.A., *supra*, may be useful for this purpose. Failure to provide the court with sufficient evidence regarding the blockchain's reliability may prevent the court from taking judicial notice of the blockchain's authenticity.[77]

---

identifying the area where [the defendant] was arrested and the general layout of the block."); McCormack v. Hiedeman, 694 F.3d 1004, 1008 n.1 (9th Cir. 2012) (relying on Google Maps to determine the distance between two locations because Google Maps' accuracy could not reasonably be questioned under Rule 201).

[74] Cline v. City of Mansfield, 745 F. Supp. 2d 773, 801 n.23 (N.D. Ohio 2010) (taking judicial notice that the sun set at a particular time on a particular day based on the information available at www.timeanddate.com).

[75] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1108 (9th Cir. 2015).

[76] FED. R. EVID. 201.

[77] *See, e.g.,* Report and Recommendation, at *12–*13, Hunichen v. Atonomi LLC, 19-cv-00615, 2020 WL 1929372 (W.D. Wash., Oct. 6, 2020), ECF No. 126 (In deciding a Rule 12(b)(6) motion, declining to take judicial notice of several pieces of evidence, including blockchain records, because "Counter-defendants fail to support the proper consideration of the blockchain evidence through judicial notice or the doctrine of incorporation-by-reference. Specifically, the court is not persuaded the blockchain evidence is necessarily complete, its contents not subject to reasonable dispute or varying interpretation, and its use not improper as a defense to otherwise cognizable . . . ." The *Atonomi* court noted that, while Rule 201 permits the court to take judicial notice of a fact "not subject to reasonable dispute," FED R. EVID. 201(b), it does not permit the court to "take judicial notice of facts favorable to the moving party that could be reasonably disputed" and the opposing party in *Atonomi* did in fact dispute certain facts related to the blockchain evidence.) (internal citations omitted); *see generally* United States v. Kane, No. 2:13-cr-250, 2013 WL 5797619, at *9 (D. Nev. Oct. 28, 2013) (Expressing caution in taking judicial notice of websites because "the internet

Judicial notice of the blockchain will generally be limited to the authentication of the blockchain itself. Judicial notice does not relieve the government of its burden to explain the relevant activity or transactions on the blockchain.[78] The government will still need to provide evidence regarding those transactions to the jury, including, where relevant, evidence indicating the defendant—or some other party—was responsible for the transaction. Judicial notice simply avoids unnecessary authentication witnesses or bolsters the grounds for authentication of the blockchain evidence.

B. Overcoming hearsay concerns

The rule against hearsay prohibits the admission of an out-of-court statement "to prove the truth of the matter asserted."[79] Some legal commentators have raised concerns that courts could consider blockchain evidence inadmissible on hearsay grounds.[80] Any hearsay challenges to the admissibility of the blockchain can be readily overcome, however.[81] First, the blockchain records are not statements at all—they are electronically generated records. Second, even if the

---

contains an unlimited supply of information with varying degrees of reliability, permanence, and accessibility.") (citing Pickett v. Sheridan Health Care Center, 664 F.3d 632, 648 (7th Cir. 2011)).

[78] *See generally* Wilbon v. Plovanich, No. 12 C 1132, 2016 WL 890671, at *31–*32 (N.D. Ill. Mar. 9, 2016) (declining to take judicial notice of a Google Map because the proponent marked the map with a description of the defendant's alleged route).

[79] FED. R. EVID. 801(c)(2), 802.

[80] James Ching, *Is Blockchain Evidence Inadmissible Hearsay?*, LAW.COM (Jan. 7, 2016) ("[T]here is a potential hearsay barrier to the introduction of any result from a distributed ledger, permisionless [sic] or not and proprietary or not."); *see also* Casey C. Sullivan, *Could Blockchain Evidence Be Inadmissible?*, FINDLAW (May 5, 2016) (Summarizing Ching's arguments and noting, "It's possible that blockchain evidence may be inadmissible hearsay."); Emily Knight, *Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility Under the Federal Rule*s, 48 HOFSTRA L. REV. VOL. 519 ("The most notable question surrounding the admissibility of blockchain evidence is if the record constitutes admissible hearsay.").

[81] *Contra* Spring, *supra* note 38, at 935 ("[B]lockchain evidence is almost always inadmissible in federal court, and is only admissible under limited, factually specific scenarios. However . . . this state of affairs contradicts the very purpose of hearsay doctrine.").

blockchain records were statements, they would readily fall into one of several hearsay exceptions.

1. Not hearsay: electronically generated

As a threshold matter, records on the blockchain are not hearsay because the blockchain is electronically generated through automated processes.[82] For the purposes of the hearsay rules, a statement is defined as "a person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion."[83] Courts have widely held that machine-generated evidence is not hearsay.[84] As the court mused in *United States v. Moon*, "If [machine-produced readings] are 'statements' by a 'witness against' the defendants, then the machine must be the declarant. Yet how could one cross-examine a gas chromatograph? Producing spectographs, ovens, and centrifuges in court would serve no one's interests."[85]

---

[82] *See* Guo, *supra* note 38, at 446–47 ("Since humans do not actually generate the receipts on the blockchain, it is possible that courts will recognize distributed ledger receipts as computer-generated evidence and therefore not hearsay. Although people certainly engage directly in transferring Bitcoin to each other, records of each transaction are generated without human influence, entered automatically through a constantly-updating algorithm on every computer in the blockchain network."); Knight, *supra* note 80, at 519 ("With regard to a blockchain, courts may consider blockchain evidence to be solely computer-generated and not an assertion for the purposes of hearsay. In spite of the fact that people interact with the protocol in order to engage in a transaction, the *actual* record of the transaction, that is, the information contained in the block, is computer generated."); Justin Steffen, et al, *Lessons From A Crypto Mock Trial* (Feb. 22, 2019), https://www.icemiller.com/MediaLibraries/icemiller.com/IceMiller/PDFs/3-Lessons-From-A-Crypto-Mock-Trial.pdf (Describing the admission of blockchain evidence at a mock trial over a defense hearsay objection and noting, "Judge Blakey likened the record to a verbal or 'mechanical act' akin to the display of time on a clock, rather than an out-of-court statement.").

[83] FED. R. EVID. 801(a).

[84] *See* United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008); United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007); United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003).

[85] *Moon,* 512 F.3d at 362.

Some writers have questioned whether the blockchain is appropriately treated as machine-generated given the involvement of humans in originating the transactions.[86] As the Eleventh Circuit noted in *United States v. Lamons*, "there can be no statements which are wholly machine-generated in the strictest sense; all machines were designed and built by humans."[87] Indeed, any review of the blockchain itself would confirm that the data contained therein does not resemble any human statement, even if a human-initiated transaction underlies the data. There is a reason that law enforcement uses blockchain analysis software rather than reviewing the blockchain data by hand in its raw form.

Existing case law supports this approach. Blockchain evidence is quite similar to the transaction records the Tenth Circuit deemed non-hearsay in *United States v. Channon*.[88] *Channon* involved Excel spreadsheets containing transaction records that were created at the point of sale, transferred to the merchant's servers, and then passed to a database maintained by another party. While these records were of transactions that people conducted at the merchant's stores, the *Channon* court conclusively found that "these records were produced by machines" and were not statements for hearsay purposes.

Other fact patterns considered by courts are similarly illustrative. The Third Circuit, for example, determined that fax headers were non-hearsay machine statements[89] even though that information was necessarily derived from a human who entered the information routing the fax. Indeed, in finding the district court's decision to exclude the evidence harmless, the Third Circuit observed, "Fax

---

[86] *See* Guo, *supra* note 38, at 446–47 ("Since each transaction recorded in a distributed ledger is the direct result of human transaction—and is cryptographically signed by the "owner" of Bitcoin wallet with his private key—the amount of influence that a person has on such a machine-made assertion is arguably much larger than any possible impact someone could have on a digital photograph."); Knight, *supra* note 80, at 519 ("Given the fact that records of blockchain transactions result from human activity of, at the very least, initializing the transaction, one can opine that there is a greater amount of human impact over the machine-made blockchain record compared with the level of influence over a digital photograph.").

[87] *Lamons*, 532 F.3d at 1263 n.23.

[88] United States v. Channon, 881 F.3d 806, 811 (10th Cir. 2018).

[89] *Khorozian*, 333 F.3d at 506.

headers are easily fabricated by the sender."[90] The Eleventh Circuit determined that a data compilation of telephone calls, showing calls originating from the defendant's cell phone number, was similarly non-hearsay, despite the role of persons in initiating and receiving the calls.[91] As these cases make clear, the involvement of humans in activity giving rise to the computer-generated records does not transform the records themselves into hearsay statements.

2. Business record

Rule 803(6) permits the admission of records of regularly conducted activity as an exception to the general bar of hearsay evidence. Rule 803(6), commonly referred to as the business record exception, allows for the admission of "a record of an act, event, condition, opinion, or diagnosis" if three conditions are met: (1) "the record was made at or near the time by—or from information transmitted by—someone with knowledge;" (2) "the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;" and (3) "making the record was a regular practice of that activity."[92] The blockchain readily meets each condition.

The discussion categorizing blockchain evidence as a business record is discussed in Section III.A., *supra*. That discussion dealt with the use of a business record certification pursuant to 902(11) to authenticate blockchain evidence—which is distinct from the requirement that, once authenticated, the evidence must still be categorized as non-hearsay or fall within an exception in order to be admitted. The analysis of the categorization of the blockchain evidence as a business record is largely transferrable, however, since Rule 902(11) incorporates Rule 803(6).

3. Market report

Blockchain evidence may also fall into the hearsay exception set forth in Rule 803(17), *market reports and similar commercial publications*, which excepts "[m]arket quotations, lists, directories, or other compilations that are generally relied on by the public or by

---

[90] *Id*. at 507.

[91] *Lamons,* 532 F.3d at 1263 ("We have no difficulty concluding that the statements in question are the statements of machines, not statements of persons.").

[92] FED. R. EVID. 803(6).

persons in particular occupations."[93] Weinstein's Federal Evidence explains:

> As with other hearsay exceptions, the admissibility of market reports and commercial publications under Rule 803(17) is predicated on the two factors of necessity and reliability. Necessity lies in the fact that if this evidence is to be obtained it must come from the compilation, since the task of finding every person who had a hand in making the report or list would be impossible. Reliability is assured because the compilers know that their work will be consulted; if it is inaccurate, the public or the trade will cease consulting their product.[94]

Courts have found that the Kelley Blue Book, a New York Stock Exchange (NYSE) Trade & Bid database, a report compiling a list patents that was created by a consulting firm, a CARFAX history report, Bloomberg Market Reports, a database maintained by the National Insurance Crime Bureau (NICB), a real estate database, and LexisNexis all fall within the Rule 803(17) exception.[95]

---

[93] FED. R. EVID. 803(17).

[94] JACK B. WEINSTEIN & MARGARET A. BERGER, 5 WEINSTEIN'S FEDERAL EVIDENCE § 803.19 (2021).

[95] *In re* Penny, No. 10-55073, 2011 WL 20488, at *6 (Bankr. N.D. Cal. Jan. 21, 2011) (Determining that the Kelley Blue Book is covered by Rule 803(13), noting, "The Kelley Blue Book is objective, serves the interests of standardization and predictability, and is cost-effective, which benefits the parties."); Sec. Exch. Comm'n v. Competitive Techs., Inc., No. 3:04-cv-1331, 2006 WL 3346210, at *8 (D. Conn. Nov. 6, 2006) (NYSE Trade & Bid database); *In re* Innovatio IP Ventures, LLC, Pat. Litig., No. 11 C 9308, 2013 WL 5393609, at *177 (N.D. Ill. Oct. 3, 2013) (list of patients created by a consulting firm); Garcia v. Roy's Trucks & Equip., No. 17-CV-0950, 2018 WL 6338364, at *5 (N.D. Tex. Aug. 24, 2018) (CARFAX); *see* United States v. Masferrer, 514 F.3d 1158, 1162 (11th Cir. 2008) ("The government presented evidence at trial establishing that Bloomberg financial information is universally relied upon by individuals and institutions involved in financial markets."); United States v. Goudy, 792 F.2d 664, 674 (7th Cir. 1986) (admitting a bank directory showing the "routing number" prefix for Los Angeles); United States v. Olson, No. 94-30387, 1995 WL 746177, at *1 (9th Cir. 1995) (admitting a "Gun Trader's Guide" that indicated where a firearm was manufactured); United States v. Cassiere, 4 F.3d 1006 (1st Cir.

4. Residual exception

Even if blockchain evidence does not fall into one of the above hearsay exceptions, it is a prime candidate for inclusion under the residual hearsay exception.[96] The residual hearsay exception, set forth in Rule 807, was revised in December 2019. Under Rule 807, a hearsay statement should not be not excluded, even if it does not fall into a defined hearsay exception, if the statement is "supported by sufficient guarantees of trustworthiness" and is "more probative on the point for which it is offered" than any other evidence that can be

---

1993) (admitting the publication "County Comps," which contained data regarding the monthly listings of properties sold, the sales prices, and the dates the sales were closed); United States v. Woods, 321 F.3d 361, 364 (3d Cir. 2003) ("Because we are satisfied that the NICB database is both necessary and reliable, we conclude that it is precisely the type of evidence that Rule 803(17) envisions."); U.S. Bank, Nat'l Ass'n v. UBS Real Estate Sec. Inc., 205 F. Supp. 3d 386, 442 (S.D.N.Y. 2016) (real estate database and LexisNexis) (Determining that a "database that includes information on properties by owner and transaction history" was appropriately admitted under 803(17) where the witness "testified that he and other underwriters and re-underwriters commonly used the database as a source of information.") (Determining that records from LexisNexis were appropriately admitted under 803(17) where the witness testified that LexisNexis "provides a lot of information" to help identify fraud, and is commonly used by underwriters to identify fraud."). *But see* In re C.R. Bard, Inc., 810 F.3d 913, 924 (4th Cir. 2016) (A Material Data Safety Sheet (MSDS) was not appropriately admitted under 803(17) where a party "sought to use a portion of the MSDS that was not factual but rather operated as a warning and disclaimer of liability for the self-interested issuing party. The warning from Phillips that polypropylene should not be used in human implants was an opinion the company issued within the MSDS for self-interested reasons, and it therefore bears no resemblance to the factual, list-type documents enumerated in Rule 803(17)."); Shepherd v. Am. Broad. Cos., 862 F. Supp. 505, 508 n.13 (D.D.C. 1994) (Rejecting the argument that legal fee surveys published in the *Legal Times* were admissible under 803(17) because, "The court is not yet convinced that published fee surveys reliably reflect rates actually billed and not rates that surveyed lawyers have artificially inflated for the *Legal Times* audience.").

[96] *C.f.* Spring, *supra* note 38, at 944 ("[W]hile the residual exception is currently the best method to admit blockchain evidence, on policy grounds, it is not a particularly good one," instead proposing an amendment to the Federal Rules of Evidence to allow for the admission of blockchain evidence.).

reasonably obtained.[97] In assessing the guarantees of trustworthiness, the court should consider any corroborating evidence as well as "the totality of circumstances" in which the statement was made.

The residual exception should be used only where a hearsay statement cannot be admitted under another exception.[98] Since blockchain evidence should not be considered hearsay at all, and even if it were, it would fall into one of several exceptions discussed *supra*, prosecutors will rarely need to invoke the residual exception. It is, however, available as a lifeline if needed.

5. Specific transactions may fall outside of hearsay preclusion

Even if a court were to find that transactions are statements that do not fall into one of the above exceptions, specific transactions would be admissible. If transactions are statements, then transactions conducted by the defendant would be admissible as statements of a party opponent. Transactions conducted by co-conspirators as part of the criminal scheme would similarly be admissible. Victims, undercover agents, or other transaction counterparties could testify to their own transactions.

C. Confrontation Clause issues

The Confrontation Clause of the Sixth Amendment generally bars the admission of testimonial hearsay in a criminal case where there is no opportunity for cross-examination.[99] A statement is considered testimonial for Sixth Amendment analysis when its "primary purpose . . . is to establish or prove past events potentially relevant to later criminal prosecution."[100]

---

[97] FED. R. EVID. 807.

[98] FED. R. EVID. 807 advisory committee's notes to 2019 amendment ("[T]he opponent cannot seek admission under Rule 807 if it is apparent that the hearsay could be admitted under another exception."). *Contra id.* ("A court is not required to make a finding that no other hearsay exception is applicable.").

[99] Crawford v. Washington, 541 U.S. 36, 59 (2004) ("Testimonial statements of witnesses absent from trial have been admitted only where the declarant is unavailable, and only where the defendant has had a prior opportunity to cross-examine.").

[100] Davis v. Washington, 547 U.S. 813 (2006).

This generally will not pose an issue for blockchain evidence because, as discussed *infra*, the records are not hearsay because they are machine generated; and even if they were hearsay, they would be non-testimonial as business records and not created in anticipation of litigation.[101]

As the Eleventh Circuit observed in *United States v. Lamons*, "the witnesses with whom the Confrontation Clause is concerned are *human* witnesses."[102] As Judge Grimm, a renowned electronic evidence expert and jurist, noted, "while [a] machine output might be prepared for litigation, *it is not testimonial because it is not hearsay*. Machines do not make statements, and cannot be cross-examined; and the Confrontation Clause applies only to statements that are hearsay."[103] Additionally, as the Supreme Court noted in *Crawford v. Washington*, certain categories of hearsay exceptions, including business records, are non-testimonial by their nature.[104]

If the government uses certifications under Rule 902 to authenticate the evidence, prosecutors should be mindful of the manner in which the certifications are drafted and their treatment in court to avoid any Confrontation Clause issues. A more fulsome discussion of Confrontation Clause considerations specific to electronic evidence certifications is included in *Authenticating Digital Evidence* within the February 2019 edition of this publication.[105] Courts are primarily concerned with Confrontation Clause issues arising from certifications of data where the data itself—not just the certificate attesting to the

---

[101] *C.f.* Guo, *supra* note 38, at 444–45 ("[B[lockchain evidence, as an out-of-court 'assertion' utilized to prove the truth of the matter, would probably be subject to both hearsay scrutiny and possibly Confrontation Clause analysis.") (citing U.S. v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015)); *Id.* at *13 n 1.

[102] United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008).

[103] Grimm, *supra* note 61, at 49.

[104] *Crawford*, 541 U.S. at 56; *see also* Tran v. Roden, 847 F.3d 44, 51 (1st Cir. 2017) ("[B]usiness records [are not] testimonial as long as they are not created for the purpose of prosecution.") United States v. Forty-Febres, No. 16-330, 2018 WL 2182653, at *6–*7 (D.P.R. May 11, 2018) ("The registration records at issue are non-testimonial business records that were not created for the purpose of prosecution, but created in the ordinary course of DTOP's business.").

[105] Levy & Haried, *supra* note 49, at 86–93.

data's authenticity—was created for use at trial.[106] Because the blockchain records themselves—albeit not the certifications—were created before and apart from litigation, they generally will not raise Confrontation Clause issues.[107] And where the certification is not presented to the jury but instead is used to satisfy a judge's criteria for admission before introducing the records through the testimony of a live witness, no Confrontation Clause issues arise.[108]

D. Presenting the trial testimony

In considering trial testimony involving blockchain evidence, prosecutors are advised to consider *what* evidence to present, *who* to present the evidence through, and *how* to present it.

1. What to present

Prosecutors should think carefully about exactly what evidence they need to present to the jury and how they can streamline or simplify that presentation. Case teams often default to telling the story based on how the investigation developed chronologically, but this is frequently not the most effective approach for trial presentation.

In many instances, prosecutors will not have to rely on the blockchain at all when presenting evidence in a virtual currency case. Prosecutors may be able to tell a compelling story based on business records from virtual currency exchanges, testimony of victims, or electronic evidence recovered from defendant's devices or online accounts. For example, in *United States v. Brown*, where the

---

[106] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 322–23 (2009) (recognizing that a custodian "could by affidavit *authenticate* or provide a copy of an otherwise admissible record, but could not . . . *create* a record for the sole purpose of providing evidence against a defendant").

[107] Grimm, *supra* note 61, at 50 ("So at the very least, Rule 902(13) certifications would . . . be properly admitted in the large number of situations in which the authenticated information was generated before the litigation arose.").

[108] *See id.* at 50–51 & n.143 ("The government may well opt to use the certificate to pass the admissibility threshold with the judge, and then establish its authenticity to the jury (if challenged, as it often is not) by way of a witness, who will likely provide a more interesting presentation than a certificate ever could. When the government makes that decision, the certificate raises no constitutional concerns because it is not admitted at trial and so the declarant is not a "witness against" the defendant.").

defendant attempted to extort a victim for a demand in bitcoin, the government introduced evidence of the ransom demand listing a specific Bitcoin address and introduced internet history evidence recovered from the defendant's computer showing that he checked that address' balance on a popular open-source blockchain explorer.[109] This was significant because the address was previously unused and, therefore, should have been known only to the perpetrator and the recipient of the ransom demand. Coupled with additional testimony providing this background and context for the uniqueness of a bitcoin address, this evidence would allow a jury to understand the significance of the defendant's interest in the ransom address separate from any blockchain-based presentation. Prosecutors should consider whether admitting records from the blockchain itself is truly necessary.

Often, cases that involved extremely complex blockchain analysis in the investigative stage can be told in a much simpler fashion by the time the case arrives at trial. Consider, for example, a 2017–2018 investigation into a website selling access to child exploitation material and accepting payment in bitcoin. Using blockchain analytics software, law enforcement identified the cluster of bitcoin addresses associated with the website.[110] Law enforcement further noted transactions sent to the website from Coinbase, a U.S.-based virtual currency exchange.[111] Using that cluster analysis, law enforcement sent a subpoena to Coinbase, which produced customer information that allowed law enforcement to identify individuals buying child exploitation material on the site.[112] Several months later, law enforcement seized the servers hosting the website.[113] A forensic review of those servers revealed the same bitcoin addresses contained

---

[109] Transcript at 98, United States v. Brown, 13-cr-118 (M. D. Tenn. May 10, 2016), ECF No. 177.

[110] Decl. Daniels in Support of Opp. Mtn. to Suppress at 6, United States v. Jung, No. 18-cr-00482 (N.D. Cal. June 4, 2019), ECF No. 30; Decl. Meyer in Support of Opp. Mtn. to Suppress at 3, United States v. Jung, No. 3:18-cr-00482, (N.D. Cal. June 4, 2019), ECF No. 29.

[111] Decl. Meyer in Support of Opp. Mtn. to Suppress at 4, United States v. Jung, No. 18-cr-00482, (N.D. Cal. June 4, 2019), ECF No. 29.

[112] *Id*. at 3.

[113] *Id*.

in the cluster from the earlier blockchain analysis.[114] Had this case gone to trial, the prosecutor could have bypassed explaining the details of cluster analysis entirely and, instead, simply introduced evidence of the bitcoin addresses found on the server when it was seized. Similarly, the prosecutor could have used the business records produced by Coinbase, which showed a transaction from the defendant's account to one of the bitcoin addresses located on the seized server,[115] rather than introduce the underlying blockchain evidence. In this way, the trial presentation could be quite straightforward, despite the more intricate process that led investigators to identify the defendant. Similar scenarios play out quite often in cases involving blockchain analysis, where a defendant initially may be identified in part through blockchain analysis, but a search of his electronic devices or accounts may provide alternative sources of evidence that obviate the need to introduce and explain more complicated blockchain analysis to a jury.

2. Who to present

This article devotes considerable attention to the grounds for admitting blockchain information in a self-authenticating form.[116] In practice, though, parties offering blockchain-related evidence at trial will want a witness to explain to the jury the fundamentals of virtual currency and blockchain analysis. This allows a jury to better understand the evidence and its context.

For a short trial with straightforward evidence, prosecutors may opt to introduce everything through the case agent. Even when the evidence is more complicated and involved, a case agent who is well versed in virtual currency may be highly effective in explaining the relevant concepts to the jury. For example, in *United States v. Ulbricht*, the trial of the administrator of the Silk Road darknet marketplace, one of the case agents explained the fundamentals of bitcoin, the blockchain, private keys, and addresses, among other

---

[114] *Id.* ("[T]he bitcoin addresses on The Website server itself—obtained separately and apart from the Reactor blockchain analysis—showed the same Bitcoin addresses found in The Website Cluster created by the cluster blockchain analysis.").

[115] *Id.*

[116] *See* Section III, *supra.*

concepts.[117] Similarly, in *United States v. Costanza*—a money laundering case involving a peer-to-peer virtual currency exchanger converting narcotics proceeds—the government introduced testimony regarding bitcoin and blockchain analysis through a member of the case team.[118] The detective, who had been involved in numerous virtual currency investigations and received training on blockchain analysis, testified about the fundamentals of blockchain analysis, as well as the details of his own undercover transactions with the defendant, which were represented to be the proceeds of narcotics sales.[119]

In other instances, prosecutors may choose instead to offer testimony through a law enforcement witness who was not part of the case team. This can be particularly useful if your case agent is not as experienced with the nuances of the technology underlying virtual currency. Being a highly effective investigator is often a different skill set than being able to explain technically complicated matters to a lay jury. Most major federal law enforcement agencies have individuals whose primary work portfolio centers on virtual currencies. These individuals work extensively on virtual currency matters and often deliver internal and external trainings and presentations on virtual currency. As a result, they are particularly well equipped to explain virtual currency and the blockchain to a lay jury.[120]

In some cases, parties may opt to bring in an individual from outside of the government to explain virtual currency and the blockchain. This individual may be sourced from, *inter alia*, academia, think tanks, consulting firms, policy-making groups, a private sector bitcoin company, or even just a virtual currency enthusiast.[121] This may be

---

[117] Transcript at 1661–63, United States v. Ross Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 212.

[118] Transcript at 599, United States v. Costanzo, 17-cr-585, 2018 WL 11027104 (D. Ariz. Aug. 10, 2018), ECF No. 199.

[119] *Id.*

[120] *Id*. at 600 (providing an explanation of blockchain analysis by a member of the case team who presented briefings and presentations on virtual currency).

[121] *See generally* Guo, *supra* note 38, at 448 ("[A]n exchange programmer, an avid Bitcoin user, a programmer attempting to replicate the blockchain, a digital currency expert, or an investor could all be brought in at trial to explain the process, accuracy, and the exceptional reliability of blockchain receipts."), Knight, *supra* note 80, at 551 ("[A] litigant will have to offer

particularly helpful if the testimony does not pertain to a common virtual currency, such as Bitcoin, Ether, or Tether, but rather a more niche virtual currency with particular attributes that have significance to the investigation and may be best explained by someone particularly well versed in the nuances of that technology.

The choice to have the "Blockchain 101" testimony delivered through a law enforcement witness versus a private individual is one of general trial strategy and subject to varying opinions. Some prosecutors may prefer to open with a government witness who conveys a sense of knowledge and authority to the jury. The government is portrayed as in control and possessing the requisite knowledge and understanding to effectively investigate a serious crime.[122] Others may prefer instead to present the information through a "neutral" third party, whose lack of affiliation with the government may augment the perceived trustworthiness of the information.

Practice may differ by district as to whether the witness providing testimony regarding bitcoin and the blockchain needs to be noticed as an expert. This will also vary depending on whether a prosecutor is introducing the evidence through a case agent's testimony, interspersed among case-specific details, or through a separate witness specifically intended to explain virtual currency, the blockchain, clustering, or other details. The specific areas of testimony may ultimately be dispositive. In the Silk Road trial, for example, the government did not notice its government witnesses as experts. Instead, it used them to provide testimony about Bitcoin transactions, wallets, accounts, exchanges, and the blockchain, all concepts that the government noted were "familiar to any layperson who has ever used Bitcoins."[123] Similarly, the government, in *Costanzo,* introduced testimony regarding bitcoin, the blockchain, and virtual currency exchanges through a detective and an IRS agent who were not noticed

---

admissible proof of the accuracy of blockchain data in order to establish the records accuracy. This can be done by hiring an expert . . . .").

[122] *See, e.g.,* Transcript, United States v. Ulbricht, No. 14-cr-68 (S.D.N.Y. Jan. 13–15, 2015), ECF Nos. 196, 198, & 200 (A case agent testified for three days, explaining Bitcoin, the blockchain, Tor, and other concepts to the jury in addition to their relevance to the case itself.).

[123] Motion to Exclude Testimony at 5, United States v. Ulbricht, No. 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 165.

as experts.[124] While many prosecutors notice experts only where they are providing opinion testimony, there is no such restriction in Rule 702, which states that experts may testify "in the form of an opinion *or otherwise*."[125] Noticing an expert may be particularly useful when presenting clustering evidence, discussed further below in Section III.D., *infra*.

3. How to present it

Blockchain evidence can easily seem unnecessarily convoluted to even the most experienced prosecutors and agents, much less lay juries. A successful presentation to the jury will thus often necessitate distilling more complex information into more readily digestible exhibits.

In explaining the basics of virtual currency and the blockchain to the jury, parties are advised to make liberal use of demonstratives, to the extent the court will permit. Visual aids can greatly aid the jury in understanding the technical concepts presented. For example, the government, in *Silk Road*, displayed a diagram depicting a bitcoin transaction—using the iconic *Alice* and *Bob* participants—while having the case agent walk through the steps in a bitcoin transaction.[126] Careful selection of demonstrative exhibits can assist the trier of fact. Parties should be mindful when choosing demonstratives, however, to avoid those whose technical detail could confuse rather than clarify.

---

[124] Transcript at 611, United States v. Costanzo, 17-cr-585, 2018 WL 11027104 (D. Ariz. Aug. 10, 2018), ECF No. 199. The government in *Costanzo* did notice another IRS agent as an expert to testify about applicable financial regulations.

[125] FED. R. EVID. 702 (emphasis added); *see also* FED. R. EVID. 702 advisory committee's notes to proposed rules ("Most of the literature assumes that experts testify only in the form of opinions. The assumption is logically unfounded. The rule accordingly recognizes that an expert on the stand may give a dissertation or exposition of scientific or other principles relevant to the case, leaving the trier of fact to apply them to the facts."); Levy & Haried, *supra* note 49, at 93 ("Expert Witnesses do not have to testify in the form of opinion.").

[126] Transcript at 171, United States v. Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 14, 2015), ECF No. 198.

Blockchain evidence is a perfect candidate for a summary exhibit, governed by Rule 1006 of the Federal Rules of Evidence.[127] The voluminous nature of the blockchain—over 300 GB[128] and encompassing over 580 million transactions[129]—makes it the exact sort of dataset envisioned by Rule 1006. Link charts showing the flow of funds will likely be among the most useful summary exhibits in the blockchain context. For example, a link chart consistent with Rule 1006 could depict the flow of funds from an undercover's wallet to the defendant's account at a virtual currency exchange, or any other sort of transaction path that is of relevance to the prosecution. Summary charts could also include spreadsheet-style charts summarizing the defendant's blockchain activity, such as the volume and value of transactions with various counterparties. These summaries will be much more useful to the jury in understanding the blockchain evidence than the raw presentation of hundreds or thousands of individual transactions.

4. Cluster-specific considerations

Many commercial blockchain analysis tools go beyond simply clustering addresses together and provide insight into who owns or controls key clusters associated with major services. For example, in most tools, the clusters associated with particular bitcoin exchanges are labeled and attributed to those exchanges. This information is not contained within the blockchain itself. Rather, the blockchain analysis software supplements the actual blockchain data with additional analysis or data sources to be able to say that *Cluster X* is, in fact, owned by *Bitcoin Exchange Y*. This information may come from the exchange itself, from open source information, or from the blockchain analysis firm conducting transactions with the exchange.

In the case of a Bitcoin exchange, replicating this attribution in a format easily presented in court is straightforward—a subpoena to the exchange will also show that the address of interest is held by that

---

[127] FED. R. EVID. 1006 ("The proponent may use a summary, chart, or calculation to prove the content of voluminous writings, recordings, or photographs that cannot be conveniently examined in court.").
[128] *Blockchain Size (MB)*, BLOCKCHAIN.COM (Nov. 1, 2020), https://www.blockchain.com/charts/blocks-size.
[129] *Total Number of Transactions*, BLOCKCHAIN.COM, https://www.blockchain.com/charts/n-transactions-total (last visited Feb. 11, 2021).

exchange. Presenting this attribution in court, however, can be more complex for clusters that are associated with services that are not able or available to confirm their own addresses. Take, for example, a prosecution of a darknet vendor who was selling narcotics on a particular darknet market. Once the investigators knew one of the vendor's addresses (which we will assume was identified independently), they could use blockchain analysis to identify transactions between the cluster of addresses controlled by the vendor and a large cluster of addresses, *Cluster X*. The blockchain analysis tool used by the investigators would likely label *Cluster X* as owned by *Darknet Market X*. Though in order to show at trial that *Cluster X* is in fact owned by *Darknet Market X*, the government has to present evidence beyond that contained in the blockchain itself.

There are numerous ways that the government can accomplish this objective. If *Darknet Market X* was shut down, and its servers seized by law enforcement, a law enforcement witness involved in that operation may be able to testify that the addresses of interest were found on *Darknet Market X*'s servers.[130] Also, an agent who conducted undercover transactions on *Darknet Market X* would be able to testify that she funded an account at *Darknet Market X* by sending virtual currency to a particular address, and additional blockchain analysis could be presented to explain that that address was contained within the cluster that transacted with the defendant. Alternatively, prosecutors could seek to have the blockchain analysis company testify to the basis for the cluster, though such an approach is generally disfavored and discouraged by the companies themselves, both to protect the companies' trade secrets and to avoid a situation where the blockchain analysis companies are asked to field witnesses for every major virtual currency trial when a law enforcement witness would more than suffice.

Parties may also consider whether clustering evidence is best presented through an expert pursuant to Rule 702, discussed in Section III.D., *supra*. This provides for greater flexibility in witness selection, as the expert can base her testimony on data that she "has

---

[130] For example, a witness in the Silk Road trial who reviewed the site's servers testified that there were over 2 million unique bitcoin addresses found on servers seized during the takedown of the Silk Road Marketplace. Transcript at 1684–86, United States v. Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 212.

been made aware of," in addition to those that she personally observed.[131] This data need not even be admissible, provided certain requirements are met.[132] Prosecutors seeking to provide expert testimony regarding clustering, however, should be prepared for a potential *Daubert* hearing.[133] Prosecutors should develop a plan to appropriately address any trade secret or law enforcement privilege issue in advance of the *Daubert* hearing.[134]

In practice, defendants may want to stipulate to the attribution of certain clusters. A witness testifying about a particular address being associated with a particular darknet market or other criminal service will necessarily provide a fair amount of detail as to the illicit dealings of that platform. As a trial strategy, many defendants want to avoid putting more evidence before the jury regarding the nefarious activity perpetrated by groups linked to the defendant. Such stipulation has the added benefit of saving trial witnesses, who may need to travel from out of district at considerable expense and whose testimony would add to the length of the trial. Similarly, in some cases, certifications under 902(13) or 902(14) can help streamline the presentation of evidence about cluster attribution.

E. Discovery

The existence of blockchain-related evidence does not change a prosecutor's substantive discovery obligations. There are, however, some specific issues that warrant additional attention from the prosecutor.

While producing discovery, prosecutors should consider the extent of the blockchain evidence they will seek to admit at trial. If the evidence is likely to be constrained to discrete transactions that were analyzed by the case team, discovery may be relatively straightforward. If,

---

[131] FED. R. EVID. 703.

[132] FED. R. EVID. 703 ("If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. But if the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.").

[133] *See* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).

[134] The particulars of preparing for a *Daubert* hearing are beyond the scope of this article, but additional useful resources are available. *See, e.g., Expert Witnesse*s, 58 U.S. ATTY'S BULL., no. 1, 2010.

however, the team envisions needing to rely on or admit voluminous records and use extensive summary charts, additional attention may need to be given to ensuring that prosecutors make the underlying data available to defense counsel, and to the court if requested.[135] In some cases—particularly in cases where the absence of transactions is as relevant as the existence of others—it may be appropriate to offer to produce a copy of the blockchain itself, or make it available for defense counsel to review.[136] In practice, defense counsel is unlikely to want to receive a 300 GB file of publicly available information.[137]

As discussed in Section III.D., *supra*, investigators may produce various charts using blockchain analysis tools over the course of their investigation. Many of these tools use a tool-specific graph format that may not be compatible with other software; as a result, the graphs may not be viewable outside of the specific software used to create them.[138] Prosecutors should anticipate this issue and develop a plan for producing the information to defense counsel. Some defense counsel who litigate extensively in blockchain matters—or, more likely, the experts they hire—may purchase licenses for the same commercial blockchain analytics tools that law enforcement uses. This scenario will streamline discovery considerably as the prosecution team can simply produce the graphs in their native file formats. In most situations, however, the prosecution team will need to consider

---

[135] FED. R. EVID. 1006 ("The proponent [of a summary chart] must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place."); Sec. Exch. Comm'n v. Competitive Techs., Inc., No. 3:04-cv-1331, 2006 WL 3346210, at *8 (D. Conn. Nov. 6, 2006)(noting that the SEC should have produced the New York Stock Exchange (NYSE) Trade & Bid Database database).

[136] FED. R. EVID. 1006 ("The proponent [of a summary chart] must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place."); *Competitive Techs., Inc.*, No. 04-cv-1331, 2006 WL 3346210, at *8 (noting that the SEC should have produced the New York Stock Exchange (NYSE) Trade & Bid Database database).

[137] Knight, *supra* note 80, at 549 ("With public blockchains, there is a limited need for discovery as the information stored can be easily viewed and accessed by a party in need of the information for his cause of action. This can be done through querying a public blockchain for relevant information via an applicable website.").

[138] This problem is not unique to blockchain data. Increasingly, law enforcement must use specific software and tools to effectively review electronic evidence.

the best alternative means to comply with its discovery obligations while making the information available to the defense. For example, the case team may consider exporting the raw data from a graph as CSV files or spreadsheets and taking screen captures of the charts. This can be a labor-intensive undertaking, and advanced planning helps simplify the process to the extent possible.

IV. Conclusion

In sum, blockchain analysis is a powerful tool that can be effectively leveraged at practically any stage of an investigation. Prosecutors handling a wide range of different types of cases may find blockchain analysis useful in identifying meritorious targets, developing probable cause to jump start an investigation, and even in proving a defendant's guilt beyond a reasonable doubt. That said, admitting blockchain analysis evidence is necessary only in a subset of cases, and prosecutors are well advised to think ahead about the various legal and practical challenges and considerations they may face when incorporating this technique into their investigative plan.

About the Authors

C. Alden Pelker is a Senior Counsel in the Computer Crime and Intellectual Property Section, where she investigates and prosecutes complex cyber criminal schemes involving the illicit use of cryptocurrency.

Christopher B. Brown is an Assistant United States Attorney in the Fraud Section, Cyber Crime Unit of the United States Attorney's Office for the District of Columbia, where he has served since 2014. He previously worked in the Office's Asset Forfeiture and Money Laundering Section and Cyber Crime Section.

Rich Tucker spent 11 years as an Assistant United States Attorney at the U.S. Attorney's Office in the Eastern District of New York, where he served as Chief of the National Security & Cybercrime Section and Senior Litigation Counsel for Cybercrime Investigations and Prosecution. In January 2021, Rich joined the secure identity company CLEAR as Senior Vice President, Legal, Privacy & Regulatory.

Prosecuting Sex Trafficking Cases in the Wake of the Backpage Takedown and the World of Cryptocurrency

Jane Khodarkovsky
Trial Attorney
Money Laundering and Asset Recovery Section
Criminal Division

April N. Russo
Assistant United States Attorney
District of Columbia

Lauren E. Britsch
Trial Attorney
Criminal Division

Over the last five years, with the Backpage takedown, the passage of the federal Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), and the rise of cryptocurrency, the landscape for investigating and prosecuting sex trafficking offenses has changed dramatically. But these investigations are more necessary now than perhaps ever before. Sex trafficking remains prevalent. In 2019, Polaris reported that the U.S. National Human Trafficking hotline received 11,500 reports of human trafficking involving 22,326 survivors, over 14,000 of whom were survivors of sex trafficking.[1] And the National Center for Missing and Exploited Children (NCMEC) noted that one in six of the 26,300 runaways reported in 2019 were likely victims of sex trafficking, a higher percentage than that of 2018.[2]

Sex trafficking of minors and adults is a worldwide problem. Though the extent of sex trafficking is hard to quantify, there is no doubt that it affects both foreign and American victims alike. A primary motivation for traffickers is the profit generated from exploiting others. According to the International Labor Organization (ILO) and the United Nations Office on Drugs and Crime (UNODC), human

[1] POLARIS, 2019 DATA REPORT 1 (2020).
[2] *See About NCMEC*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.missingkids.org/footer/media/keyfacts (last visited Oct. 7, 2020).

trafficking networks generate over $150 billion in profits around the world.[3] In 2010, sex traffickers generated more profits than Walmart and Exxon Mobil combined—the top two Fortune 500 companies that year.[4]

The federal government, all states, and the District of Columbia have criminalized human trafficking. The Trafficking Victims Protection Act (TVPA) of 2000 is the landmark federal law and the foundation of the federal response to sex trafficking.[5] It created the specific sex trafficking offenses now codified in 18 U.S.C. § 1591.[6] Over the years, the sex trafficking statutes have been amended several times in an attempt to address three identified gaps: (1) prosecuting customers or *Johns*; (2) remedies for victims; and (3) tackling the online advertisement of commercial sex.[7] For example, the Justice for Victims of Trafficking Act of 2015 (JVTA) added the verbs *patronizes* and *solicits* to the sex trafficking statute to facilitate the prosecution of customers.[8] The act also clarified that the government does not have to prove a defendant knew or recklessly disregarded that a victim was a minor if the defendant had a reasonable opportunity to observe the victim, a valuable tool against both customers and traffickers who often deny knowledge of their teenaged victims' ages.[9] The law also imposed a $5,000 special assessment for human

---

[3] *See* INT'L LABOUR OFF., PROFITS AND POVERTY: THE ECONOMICS OF FORCED LABOUR 13 (2014). The comparable estimates for the drug trade range from about $426 billion to $652 billion. *See* CHANNING MAY, TRANSNATIONAL CRIME AND THE DEVELOPING WORLD xi (2017).

[4] *See* Jacqueline Hackler, *Inconsistencies in Combatting the Sex Trafficking of Minors: Backpage's Deceptive Business Practices Should Not be Immune from State Law Claims*, 40 SEATTLE U. L. REV. 1107, 1108 (2017).

[5] Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106-386, 114, Stat. 1464.

[6] The TVPA also created additional forced labor and peonage offenses codified in Title 18, Chapter 77, of the United States Code.

[7] *See* William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, Pub. L. No. 110-457, 122 Stat. 5044; Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, 129 Stat. 227.

[8] Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, §§ 108, 109, 129 Stat. 227; 18 U.S.C. § 1591(a)(1).

[9] Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, § 108, 129 Stat. 227.

trafficking offenses to generate revenue to provide services to victims.[10]

The legal framework up until 2015 did not specifically address the online advertisement of prostitution and sex trafficking, though existing statutes had been used to target that conduct. The JVTA took the first step at specifically addressing this problem by adding the verb *advertises* to the modes of committing an offense under section 1591 when the defendant knew the victim being advertised was a minor or that force, fraud, or coercion would be used.[11] This aspect of the statute has been used primarily to prosecute traffickers and their accomplices who post online commercial sex advertisements—rather than websites that host those advertisements. As discussed below, FOSTA, signed into law in 2018, provides law enforcement with another tool to target websites that host online commercial sex advertisements.

I. Backpage

From 2008 to 2018, Backpage.com was the primary source of sex trafficking advertisements.[12] Backpage was a free online advertising service and, at one point, the second largest online classified website worldwide, with operations in 97 different countries.[13] Backpage was extremely profitable, worth over a half billion dollars at its peak. Over 90% of Backpage's income came from its "adult" advertisement section, where commercial sex ads were typically posted.[14]

Backpage undoubtedly provided an easily accessible forum for traffickers to find customers and exploit victims. Offenders could advertise their victims to tens of thousands of internet users with nothing more than $15 and a few clicks of a button on an iPhone. Because Backpage was a central hub for traffickers, consumers knew exactly where to go if they wanted to purchase sex and could quickly and easily set up the "transaction." Moreover, Backpage partnered

---

[10] *Id.* at § 101; 18 U.S.C. § 3014.

[11] Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, § 118, 129 Stat. 227; 18 U.S.C. § 1591(a)(1).

[12] *See* U.S. SENATE PERMANENT SUBCOMM, ON INVESTIGATIONS, COMM. ON HOMELAND SEC. AND GOV'T AFFS., BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX TRAFFICKING 6, 43–44 (2017) [hereinafter Backpage Knowing Facilitation].

[13] *Id.* at 1.

[14] Hackler, *supra* note 4, at 1122.

with other organizations in the prostitution industry, including websites like the Erotic Review—where consumers of commercial sex posted reviews rating prostitutes—and obtained tens of thousands of referrals from some of those organizations.[15] Thus, the existence of Backpage facilitated the proliferation of sex trafficking. In fact, in 2017, NCMEC reported that Backpage was involved in over 70% of all reports it received about the sex trafficking of minors.[16] Backpage profited immensely from these types of advertisements, earning over 500 million dollars in prostitution-related revenue from 2004 to 2018.[17]

In January 2017, after a U.S. Senate investigation found that Backpage knowingly facilitated sex trafficking and repeatedly concealed evidence of those crimes, Backpage shut down its "adult" advertisement section.[18] A little over a year later, a grand jury returned a 93-count indictment against Backpage's creators, an executive vice president of one of Backpage's parent companies, its chief financial officer, its sales and marketing director, its operations manager, and its assistant operations manager. The indictment alleged sex trafficking, money laundering, and conspiracy to commit money laundering, among other offenses. And a week after the indictment, U.S. law enforcement authorities seized Backpage and shut the website down.[19]

Backpage's shutdown was heralded as a major victory in the fight against sex trafficking by prosecutors, law enforcement, and anti-trafficking groups alike. It was not, however, without controversy.[20] The fact that the commercial sex market was

---

[15] Superseding Indictment at 11–12, United States v. Lacey, No. 18-CR-422, 2018 WL 4953275 (D. Ariz. Oct. 12, 2018), ECF No. 230.

[16] BACKPAGE KNOWING FACILITATION, *supra* note 12, at 6 & n.23.

[17] Superseding Indictment, *supra* note 15, at 1.

[18] BACKPAGE KNOWING FACILITATION, *supra* note 12, at 16–17; *Backpage.com Shuts Down Adult Section Amid Sex-Trafficking Accusations*, ABC7 L.A., (Jan. 10, 2017), https://abc7.com/backpage-backpagecom-sex-trafficking-adult-classifieds/1695059/.

[19] Sarah Lynch & Lisa Lambert, *Sex Ads Website Backpage Shut Down by U.S. Authorities*, REUTERS (Apr. 6, 2018), https://www.reuters.com/article/us-usa-backpage-justice/sex-ads-website-backpage-shut-down-by-u-s-authorities-idUSKCN1HD2QP.

[20] Along with some of the law-enforcement challenges discussed herein, many voiced their concerns that Backpage's shutdown eliminated a reliable source

centralized on a public, U.S.-based website like Backpage had in some ways made it easier for law enforcement to know where to begin a sex trafficking investigation. Law enforcement had the same access to the website as did consumers and could analyze advertisements for depictions of minors or descriptions that indicated exploitation. They used the data in the advertisements and information provided in response to subpoenas to locate offenders and victims and to set up undercover operations. Evidence from Backpage often corroborated victims' accounts or offenders' statements. Additionally, if a case went to trial, prosecutors could authenticate and admit evidence obtained from Backpage, including advertisements of sex-trafficking victims, by having a representative from Backpage testify or introducing a business record certification.

II. Post-Backpage

Five days after Backpage's seizure, FOSTA became law.[21] FOSTA makes it a criminal offense to own, manage, or operate "an interactive computer service," including websites, "with the intent to promote or facilitate the prostitution of another person."[22] The maximum penalty for a violation is ordinarily 10 years' imprisonment.[23] For an "aggravated violation," however—one involving either (1) "promot[ing] or facilitat[ing] the prostitution of 5 or more persons; or (2) act[ing] in reckless disregard of the fact that such conduct contributed to sex trafficking, in violation of 18 U.S.C. § 1591(a)"—offenders face up to 25 years' imprisonment.[24] Restitution is mandatory, and the law specifically provides that victims can recover damages and reasonable attorney's fees in a civil action as well.[25] Importantly, where the

---

of income for sex workers and made their jobs even riskier. *See, e.g.,* Megan Cassidy & Richard Ruelas, *Sex Workers 'Devastated,' Look to Alternatives After Backpage Closure*, ARIZ. REPUBLIC (Apr. 12, 2018), https://www.azcentral.com/story/news/local/arizona-investigations/2018/04/12/sex-workers-seeking-alternatives-other-websites-after-backpage-closure/507900002/.

[21] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (FOSTA incorporating the Senate's proposed Stop Enabling Sex Traffickers Act (SESTA)).

[22] 18 U.S.C. § 2421A(a).

[23] *Id.*

[24] 18 U.S.C. § 2421A(b).

[25] 18 U.S.C. § 2421A(c)–(d).

violation is not premised on section 1591(a), a defendant must assert an affirmative defense and demonstrate by a preponderance of the evidence that the promotion or facilitation of prostitution is legal in the jurisdiction where the promotion or facilitation was targeted.[26]

The takedown of Backpage had a ripple effect. Some websites that engaged in similar activity shut down for fear of similar prosecution, while others saw the shutdown as an opportunity and picked up where Backpage left off, with several moving their operations abroad. Thus far, no dominant player has captured the breadth of the marketplace like Backpage. Instead, the online commercial sex market is fractured, with dozens of different websites facilitating and profiting from online commercial sex. Several of these websites tried to reach Backpage's previous customers by using *backpage* in their domain names. For example, "backpage.ly," "ebackpage.com," "ibackpage.com," and "yesbackpage.com" emerged. A report by ChildSafe.AI—an artificial intelligence platform geared towards protecting kids from online predators—surveyed the post-Backpage landscape and predicted that the volatility in the market would continue into the near future.[27]

Compounding the challenge of a fragmented market is that many of the servers for these sites are hosted in foreign countries. This makes it more difficult for law enforcement to identify and locate the servers, to shut down the sites, and to seize relevant evidence. For example, sites like Rubmaps and EroticMonkey moved their infrastructure to Europe and switched their domains to Swiss ".ch."[28] Gathering evidence related to these sites and others operating abroad will likely require the use of Mutual Legal Assistance Treaty (MLAT) requests,

---

[26] 18 U.S.C. § 2421A(e). There is no such affirmative defense available if the offense charged is based on the defendant's conduct contributing to sex trafficking. 18 U.S.C. § 2421(e), (b)(2).

[27] ROB SPECTRE, BEYOND BACKPAGE: BUYING AND SELLING SEX IN THE UNITED STATES ONE YEAR LATER (n.d.). This article does not endorse the findings of this report as the U.S. Department of Justice (Department) was not involved in the research or analysis of the data in this report.

[28] Lalita Clozel, *After Backpage, U.S. Investigates Massage, Escort Websites That Now Dominate Market*, WALL ST. J. (Sept. 15, 2019), https://www.wsj.com/articles/after-backpage-u-s-investigates-massage-escort-websites-that-now-dominate-market-11568548800. Notably, these sites, as well as Eros.com, are linked to a Swiss businessman who was previously convicted in France of profiting from prostitution.

depend on the cooperation of the country where the servers are hosted, and require significant coordination within U.S. law enforcement.

The first federal criminal charges under FOSTA were brought in the Northern District of Texas against Wilhan Martono, the owner and operator of cityxguide.com. After Backpage was shut down, some users described CityXGuide as "taking over where Backpage left off."[29] In June 2020, U.S. law enforcement seized CityXGuide and its related websites.[30] A grand jury returned a 28-count indictment that included charges for violations of 18 U.S.C. § 2421A and alleged that CityXGuide allowed brothels, pimps, and prostitutes to advertise sexual services.[31] Law enforcement also identified multiple minor victims allegedly advertised on CityXGuide.[32] Notably, in January 2021, the court issued an order upholding the constitutionality of FOSTA and rejecting Martono's First-Amendment challenges for vagueness and overbreadth.[33]

III. Tools for proactively investigating human trafficking cases in a post-Backpage world

A. Hobbyists and sugar daddy websites

Understanding models that do not explicitly involve advertising commercial sex but are nonetheless used to facilitate it is crucial to fighting sex trafficking in a post-Backpage world. For example, ChildSafe.AI noted the increased prominence of *hobby board* and *sugar daddy* websites.[34] As described by ChildSafe.AI's report, hobby

---

[29] Press Release, U.S. Immigr. and Customs Enf't, ICE HSI Dallas Leads Investigation to Shut Down Website Promoting Prostitution and Sex Trafficking, Indictment of Owner (June 19, 2020).

[30] *Id.*

[31] Indictment, United States v. Martono, No. 20-cr-274 (N.D. Tex. June 2, 2020), ECF No. 1.

[32] Press Release, *supra* note 29.

[33] Order, United States v. Martono, No. 20-cr-274 (N.D. Tex. Jan. 5, 2021), ECF No. 28.

[34] SPECTRE, *supra* note 27. The terms "advertising," "hobby board," and "sugar dating" describe different platforms in the online commercial sex marketplace. None of these is a legal term of art, however, and therefore, these terms are not relevant to a determination of criminality.

boards are forums for *hobbyists*—consumers of commercial sex—to post reviews of the providers of commercial sex.[35] These reviews often contain pricing and contact information for providers, thus operating effectively as advertisements for their services. Hobby boards are not new, but they appear to be growing in popularity after Backpage's shutdown. Two notable examples are Rubmaps, a review site focused on massage parlors, and EroticMonkey, which focuses on escort reviews.[36]

Sugar daddy websites are another genre rising in popularity. They ostensibly offer dating services for those looking for mutually beneficial relationships. But online discussions indicate that traditional escorts—that is, prostitutes—are marketing their services within the sugar daddy model. And some of the *sugar babies* on the website are no doubt under the age of 18. For example, in March 2017, a 53-year-old man was charged with meeting a 14-year-old girl on the sugar daddy website SeekingArrangement.com and paying her to have sex in a hotel room.[37]

Targeting the distribution layer of hobbyists is one way to disrupt the developing commercial sex market on these hobby boards and sugar daddy websites. As Rob Spectre of ChildSafe.AI states, "Buyers need to feel a credible risk . . . . If no one got arrested, no buyer would be deterred."[38] Deterring buyers who are hobbyists, in turn, deters the posting of reviews—effectively advertisements—on websites, which can significantly impact the market for commercial sex. ChildSafe.AI's analysis of hobbyists showed that they are more likely to be repeat customers than buyers on traditional advertising sites.[39] Though data is limited, prosecuting consumers of commercial sex can be a deterrent and help reduce demand. For example, ChildSafe.AI observed a 56% drop in traffic on RubMaps shortly after the arrest of almost 200

---

[35] *Id.*

[36] *Id.*

[37] Press Release, U.S. Dep't of Justice, Culpeper Man Pleads Guilty to Charges of Commercial Sex with a Minor and Production of Child Pornography (Sept. 26, 2017); Affidavit in Support of Crim. Complaint and Arrest Warrant, United States v. Daniel, No. 17-cr-110 (E.D. Va. Mar. 28, 2017), ECF No. 2.

[38] Tina Rosenberg, *A.I. Joins the Campaign Against Sex Trafficking*, N.Y. TIMES (Apr. 9, 2019), https://www.nytimes.com/2019/04/09/opinion/ai-joins-the-campaign-against-sex-trafficking.html.

[39] SPECTRE, *supra* note 27.

individuals related to their patronizing Florida massage parlors.[40] Ultimately, the goal is to make it too costly for these website owners to operate in this space. One way to do that is to deter hobbyists from posting the reviews that generate the customer base and, thus, the revenue for the sites.

B. State and local law enforcement

While FOSTA created an additional federal statute for law enforcement to target online advertisers, its most important change was the removal of section 230 immunity from *state* prosecution for online advertisers of prostitution.[41] The Communications Decency Act, 47 U.S.C. § 230—passed in the early days of the evolution of the internet—immunizes internet providers for content published on their forums by third parties. FOSTA created an exception for the enforcement of sex trafficking laws.[42] Now, state and local authorities can prosecute companies that facilitate advertising prostitution in their communities. This is a significant expansion in law enforcement resources to fight an increasingly complex and ever-changing online sex trafficking industry.

Our local partners can provide valuable insight into how online advertising websites affect their communities. For example, local vice police units that recover minor victims of sex trafficking can determine if a particular victim was advertised online and, if so, on which sites. They can then identify trends and target the websites putting minors at risk in their communities. FOSTA now allows local authorities to use existing prostitution laws to prosecute operators of those sites. Federal law enforcement can support such prosecutions by assisting with MLAT requests for evidence, which is increasingly housed abroad. Federal investigators and prosecutors can also conduct parallel investigations—in particular, federal money laundering investigations, as discussed below—that support the state or local prosecutions.

---

[40] *Id.*

[41] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, § 4, 132 Stat. 1253.

[42] *See* 47 U.S.C. § 230(e)(5).

C. Public–private partnerships

Various organizations offer digital tools and databases that law enforcement can use to analyze advertisements and hobbyist reviews related to commercial sex. These databases often provide information about website users, including the location of the poster, email addresses, and telephone numbers. They can also provide invaluable information about the victims being advertised, such as whether the victims' images appear on different websites.

The most well-known of these tools is Spotlight, which is run by the non-profit organization THORN. Spotlight enables law enforcement to collaborate nationally to identify victims, who may be transported from one location to another or are advertised on platforms on the dark web.[43] Not as well-known is MEMEX,[44] a program developed by the Defense Advanced Research Projects Agency (DARPA) for anti-trafficking efforts.[45] Yet another program, Tellfinder,[46] uses artificial intelligence to analyze dark web content and identify visual patterns in advertisements, including identifying the use of the same image on different review and discussion boards. Tellfinder then provides the reconstructed advertisements, along with the e-mail addresses, telephone numbers, and other identifiers for those who uploaded the images to law enforcement.[47] Not only does this resource enable law enforcement to cross reference different websites (where the same traffickers are posting advertisements), thus demonstrating the amount of money traffickers spend to promote the exploitation of victims, which can help determine mandatory forfeiture and

---

[43] According to Thorn, Spotlight helped identify 17,092 child victims of human trafficking between 2016 and 2020. *Spotlight Helps Find Kids Faster*, THORN, https://www.thorn.org/spotlight/ (last visited May 6, 2021).

[44] MEMEX sought to enhance online search capabilities by using technology for "improved content discovery, information extraction, information retrieval, and user collaboration." *Memex (Archived)*, DEFENSE ADVANCED RSCH. PROJECT AGENCY, https://www.darpa.mil/program/memex (last visited May 6, 2021).

[45] *Id.*

[46] Tellfinder Alliance's founding partners are the New York County District Attorney's Office and Unchartered. *See TellFinder Alliance: Collaboration Across Borders and Sectors*, TELLFINDER ALLIANCE, https://www.tellfinderalliance.com/about-us (last visited May 6, 2021).

[47] *Id.*

restitution amounts,[48] it can also help identify victims and provide evidence connecting the traffickers to the victims.

"Traffic Jam," created by Marinus Analytics, is another "tool used by law enforcement across the United States, Canada, and the United Kingdom to identify sex-trafficking victims and dismantle organized criminal networks."[49] Traffic Jam analyzes data from publicly available online advertisements and cross references the information in those ads with other datapoints to illuminate patterns in traffickers' activity. In 2019, federal law enforcement used Traffic Jam to identify a trafficking network out of the District of Oregon that exploited Chinese foreign nationals for commercial sex in 12 U.S. cities and Toronto, Canada.[50] In *United States v. Chen*, five defendants were charged with interstate and foreign travel or transportation in aid of racketeering enterprises, in violation of 18 U.S.C. § 1952, for operating a sex trafficking organization in the United States, Canada, and Australia.[51] The investigation also led to charges against Hui Ling Sun, who pleaded guilty to one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h).[52] In addition, the FBI seized the primary website used to advertise the victims, www.supermatchescort.com, and 500 associated domains.

Other technology companies are also increasingly engaged in anti-trafficking efforts. For example, in May 2020, the Organization for Security and Cooperation in Europe (OSCE) and the Tech Against Trafficking coalition published a report called *Leveraging Innovation to Fight Trafficking in Human Beings: A Comprehensive Analysis of*

---

[48] Forfeiture and restitution are mandatory for all sex trafficking and forced labor offenses pursuant to 18 U.S.C. §§ 1594 and 1593, respectively.

[49] *The Role of Technology in Countering Trafficking in Persons: Hearing Before the Subcomm. on Investigations & Oversight and Subcomm. on Research & Technology of the H. Comm. On Science, Space and Technology* (Testimony of Emily Kennedy).

[50] *Id.*

[51] *See* United States v. Chen et al., No. 18-CR-559 (D. Or. Nov. 15, 2018).

[52] *See* United States v. Sun, No. 18-CR-557 (D. Or. Feb. 4, 2021). Sun is not alleged to be an owner, operator, or manager of the websites but instead pleaded guilty to collecting funds from others involved in prostitution and delivering the funds for the purpose of laundering the money to China. Plea Agreement, United States v. Sun, No. 18-CR-557 (D. Or. Feb. 24, 2021), ECF No. 45.

Technology Tools.[53] The report explored how to better leverage data and analytics from the private sector and non-governmental organizations to help law enforcement.[54] Similarly, the MIT Lincoln Laboratory—a non-profit, federally funded research and development center (FFRDC)—has used data science, machine learning, and digital evidence analytics to assist human trafficking investigations.[55] The Lincoln Laboratory also developed a "Human Trafficking Technology Roadmap" for the U.S. Department of Homeland Security's Science and Technology directorate, which seeks to fight human trafficking by pursuing evidence-based research.[56]

More resources, guidance, and funding are necessary to bridge the gap between the volume of data and the complexity of heterogenous human trafficking networks. In particular, uniform guidance to law enforcement about which private–public partnerships are available, verified, and endorsed by the Department or its law enforcement partners could enhance the ability of investigators and prosecutors to leverage analytical tools.

---

[53] ORG. FOR SEC. AND CO-OPERATION IN EUROPE & TECH AGAINST TRAFFICKING, LEVERAGING INNOVATION TO FIGHT TRAFFICKING IN HUMAN BEINGS: A COMPREHENSIVE ANALYSIS OF TECHNOLOGY TOOLS (2020).

[54] In a July 28, 2020 written statement to U.S. Congressional Committee on Science, Space, and Technology's (116th Congress) Subcommittee on Research and Technology and the Subcommittee on Investigations and Oversight, Hannah Darton of Tech for Trafficking stated that the government only accounts for a small percentage of technology efforts and initiatives, with the two main stakeholders being private sector companies and NGOs. TECH AGAINST TRAFFICKING, THE ROLE OF TECHNOLOGY IN COUNTERING TRAFFICKING IN PERSONS 5 (2020).

[55] The Role of Technology in Countering Trafficking in Persons: Hearing Before the Subcomm. on Rsch. and Tech. and Subcomm. on Investigations and Oversight of the H. Comm. on Sci., Space, and Tech., 116th Cong. 1 (2020) (prepared testimony of Matthew Daggett).

[56] *See id.* at 2 & n.1 (citing H.J.D. REYNOLDS ET AL., HUMAN TRAFFICKING SYSTEMS ANALYSIS (2019)); M.P. DAGGETT ET AL., THE HUMAN TRAFFICKING TECHNOLOGY ROADMAP: A TARGETED DEVELOPMENT STRATEGY FOR THE DEPARTMENT OF HOMELAND SECURITY (2019); Press Release, U.S. Dep't of Homeland Sec., S&T Combatting Human Trafficking Using Social Science (Jan. 30, 2019).

D. Proactive financial human trafficking investigations

Federal prosecutors have a wide range of tools to proactively combat trafficking from a financial angle. In December 2017, the Financial Crimes Enforcement Network (FinCEN) strengthened its public–private partnerships to combat human trafficking, including by mapping human trafficking networks with the use of financial analysis.[57] Under the Bank Secrecy Act (BSA),[58] financial institutions, including money service businesses (MSBs), casinos, and virtual currency exchanges, 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.[59] They make these reports by filing Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), and other reports pursuant to their BSA obligations. In 2018, FinCEN updated its SAR form to include a checkbox for financial institutions to identify suspicious activity related to human trafficking.[60] In October 2020, FinCEN released a supplemental advisory on human trafficking, which provides additional red flags for financial institutions to better identify and report indicia of human

---

[57] The FinCEN Exchange program aimed to "enhance information sharing with financial institutions," including on issues of human trafficking. Press Release, U.S. Dep't of the Treasury Fin. Crimes Enf't Network, FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing (Dec. 4, 2017).

[58] 31 U.S.C. § 5311.

[59] *See* 31 U.S.C. §§ 5311–5330; 31 C.F.R. Ch. X (formerly 31 CFR Part 103); *see also Statutes and Regulations,* FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-regulations (last visited May 31, 2021).

[60] *See Combating Human Trafficking*, U.S. DEP'T OF THE TREASURY (Jan. 29, 2020), https://home.treasury.gov/news/featured-stories/combating-human-trafficking#:~:text=In%202018%2C%20FinCEN%20updated%20its,activity%20related%20to%20human%20trafficking.&text=The%20update%20also%20allows%20law,or%20enablers%20of%20human%20trafficking.

trafficking.[61] Law enforcement can use the data reported in SARs to help identify perpetrators and facilitators of human trafficking.[62]

To help determine when to file reports of suspicious activity, certain banks also use FinCEN's 2014 Human Trafficking Advisory[63] and the Thompson Reuters Foundation's human trafficking banking toolkit,[64] which include red flags of human trafficking such as off-peak cash deposits, lack of payroll deposits, frequent use of ride share services, airfare, or Airbnb payments when those activities do not appear consistent with a customer's known occupation or residence. Data collected by FinCEN should be used by investigators to develop traffickers' financial profiles to support possible money laundering charges, even if a substantive human-trafficking offense is not charged.

Money laundering can entail concealing an illegal source of income, often so that it can be spent without raising suspicion or used to further a criminal activity or scheme (commonly referred to as *promotion* money laundering). In some cases, money launderers take *dirty* money and comingle it with *clean* money to advance their criminal enterprise and evade law enforcement detection. There are several potential money laundering charges that human trafficking prosecutors should be aware of, including the basic and international money laundering provisions of 18 U.S.C. §§ 1956(a)(1) and (a)(2); the "spending statute" of 18 U.S.C. § 1957; structuring, in violation of

---

[61] U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, SUPPLEMENTAL ADVISORY ON IDENTIFYING AND REPORTING HUMAN TRAFFICKING AND RELATED ACTIVITY (2020).

[62] It is important to note that Suspicious Activity Reports (SARs) are confidential. *See* 31 U.S.C. § 5318(g)(2); 31 CFR §§ 1020.320(e), 1021.320(e), 1022.320(d), 1023.320(e), 1024.320(d), 1025.320(e), 1026.320(e).

[63] U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, GUIDANCE ON RECOGNIZING ACTIVITY THAT MAY BE ASSOCIATED WITH HUMAN SMUGGLING AND HUMAN TRAFFICKING—FINANCIAL RED FLAGS (2014).

[64] On May 2, 2017, Thomson Reuters Foundation announced the launch of a toolkit to tackle human trafficking with financial data, sharing red flag indicators tailored specifically to European financial institutions to detect and report suspicious patterns in financial activity linked to human trafficking. *5 Ways Thompson Reuters is Making a Global Impact*, THOMPSON REUTERS, https://www.thomsonreuters.com/en/careers/careers-blog/5-ways-thomson-reuters-is-making-a-global-impact.html#:~:text=The%20Thomson%20Reuters%20Foundation%20launched,by%20the%20Thomson%20Reuters%20Foundation (last visited Oct. 9, 2020).

31 U.S.C. § 5324; operating unlicensed money transmitting businesses, in violation of 18 U.S.C. § 1960; and conspiracy to commit either section 1956 or section 1957 offenses, in violation of section 1956(h). Specifically, money laundering, in violation of 18 U.S.C. § 1956(a)(1) makes it a crime to knowingly conduct, or attempt to conduct, a "financial transaction" with proceeds from a "specified unlawful activity" (SUA). SUAs[65] are defined in 18 U.S.C. § 1956(c)(7)(A) as any act or activity constituting an offense under section 1961(1), which includes sex trafficking, in violation of section 1591; promotion or facilitation of prostitution, in violation of section 2421A (FOSTA); Interstate Travel in Aid of Racketeering (ITAR/Travel Act), in violation of 18 U.S.C. § 1952; and child sexual exploitation offenses.

Federal prosecutors should consider the facts and evidence in their cases to determine if traffickers, members of their networks, or in cases like Backpage and CityXGuide,[66] owners or operators of an online advertising website that facilitates or profits from prostitution, sex trafficking, or child exploitation could be charged with money laundering offenses. This inquiry should include, but not be limited to, determining whether the targets: (1) knowingly paid to post an advertisement for prostitution; (2) knew that the money used in a financial transaction was proceeds of an SUA; (3) used proceeds that were derived from an SUA; or (4) engaged in financial transactions with the specific intent to promote an SUA.

There have been several investigations in which prosecutors have successfully convicted operators of online platforms who violated money laundering statutes, including the prosecutions of Redbook.com, Flawlessescorts.com, and Vipescorts.com.[67] These cases

---

[65] There are other SUAs relevant to human trafficking, including all human trafficking charges under 18 U.S.C. §§ 1581–1597; sexual exploitation of children (18 U.S.C. §§ 2251, 2252, 2252A (if an actual minor), 2260); alien harboring or smuggling (8 U.S.C. §§ 1324, 1327, 1328) for financial gain; citizenship or naturalization fraud (8 U.S.C. §§ 1425, 1426, 1427); passport or visa fraud (18 U.S.C. §§ 1542, 1543, 1544, 1546), among others.

[66] In *Martono*, in addition to SESTA-FOSTA charges, the indictment charged multiple money-laundering offenses under 18 U.S.C. § 1956(a), as well as multiple Travel-Act offenses under 18 U.S.C. § 1952(a). Indictment, *supra* note 31.

[67] *See, e.g.*, Indictment, United States v. Omuro, No. 14-CR-336 (N.D. Cal. June 24, 2014), ECF No. 1 (charging Omuro with multiple counts of money

can be used as a model for prosecuting operators of other commercial sex websites for money laundering offenses in addition to potential violations of FOSTA.

IV. Cryptocurrency and its role in human trafficking

Cryptocurrency is a type of virtual currency and "is a decentralized, peer-to-peer network-based medium of value or exchange."[68] Because no company runs or controls cryptocurrency, its owners can—within seconds—conduct transactions with others around the globe. There are hundreds of different types of cryptocurrency, but the most well-known is Bitcoin. Bitcoin's invention in 2008 was the advent of the world of cryptocurrency we know today. Bitcoin's value is not tied to the value of the U.S. dollar or any other country's currency. Instead, it is derived from the value that people (its holders and its potential buyers) assign to it.[69] For this reason, the value of bitcoin

---

laundering in violation of 18 U.S.C. § 1957(a)); Judgment, United States v. Omuro, No. 14-CR-336 (N.D. Cal. June 2, 2015), ECF No. 75 (noting Omuro pleaded guilty to one count of violating 18 U.S.C. § 1952(a)(3)(A)); Information, United States v. Martin and Tameko Lindo, No. 19-CR-240 (S.D.N.Y. Apr. 8, 2019), ECF 20 (charging defendants with one count of conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h)); Letter Requesting Rescheduling of Plea Hearing, United States v. Martin, No. 19-CR-240 (S.D.N.Y. Jan. 10, 2020), ECF No. 37 (noting defendants pleaded guilty to same); Press Release, U.S. Dep't of Justice, Manhattan U.S. Attorney Announces Money Laundering Charges Against Operators Of Nationwide Prostitution Enterprise And Seizure Of Online Escort Website (July 24, 2018) (Flawless Escorts); Complaint, United States v. Reynolds, No. 20-cr-396, (S.D.N.Y. Feb. 7, 2020), ECF No. 1 (defendants charged with one count of conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h)); Press Release, U.S. Dep't of Justice, United States Attorney Announces Money Laundering Charges Against Operators Of Multimillion-Dollar Nationwide High-End Prostitution Enterprise (Feb. 11, 2020) (VIP Escorts).

[68] Michele R. Korver et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233.

[69] JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 6 (2016). To say it is derived from the value that holders and potential buyers place on it is simplifying it. There is a finite number of Bitcoins that can ever be issued, and only a certain number of Bitcoins are in circulation now, which all play into the supply and demand and ultimately the value of the currency.

has fluctuated wildly. The currency, however, has, overall, been successful—it was valued at approximately $13 in early 2013, was valued at $18,000 in early November 2020, and was valued at approximately $57,000 in early April of 2021.[70]

Owners of cryptocurrency often "access" it by using a virtual "wallet."[71] A public key (similar to a bank account) and a private key (similar to a PIN, which is used to send and receive the cryptocurrency) are used to make an exchange.[72] If a user loses their private key or cannot remember it, the value of the cryptocurrency is lost. Cryptocurrency can be traded for cash or other goods. Major retailers, including Starbucks, Whole Foods, Nordstrom, and hotel booking websites like CheapAir are among dozens of companies that now accept it.[73] Owners can also sell it in cryptocurrency exchanges, exchange it through an intermediary (such as an over-the-counter

---

[70] *See Bitcoin*, COINDESK, https://www.coindesk.com/price/bitcoin (last visited Apr. 7, 2021) (current valuation of Bitcoin); John Edwards, *Bitcoin's Price History*, INVESTOPEDIA (Feb. 3, 2021), https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp.

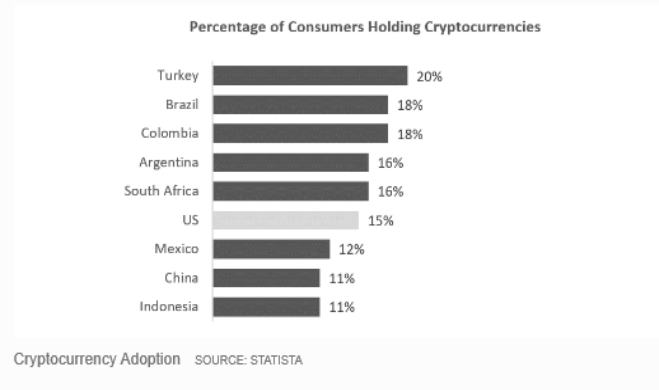
[71] Michele R. Korver et al., *supra* note 68, at 234.

[72] *Id*. at 234.

[73] Sarah Min, *Who Accepts Cryptocurrency? Whole Foods, Bed Bath & Beyond and Ulta Among Retailers*, CBS NEWS (May 3, 2019), https://www.cbsnews.com/news/who-accepts-cryptocurrency-whole-foods-bed-bath-beyond-and-ulta-among-retailers-accepting-cryptocurrency/; Michael del Castillo, *Customers Can Spend Bitcoin at Starbucks, Nordstrom, and Whole Foods, Whether They Like it or Not*, FORBES (May 13, 2019), https://www.forbes.com/sites/michaeldelcastillo/2019/05/13/starbucks-nordstrom-and-whole-foods-now-accept-bitcoin-just-dont-ask-them/?sh=1278a3ed2252; Anthony Cuthbertson, *Bitcoin Now Accepted at Starbucks, Whole Foods, and Dozens of Other Major Retailers*, INDEPENDENT (May 14, 2019), https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-stores-spend-where-starbucks-whole-foods-crypto-a8913366.html. In 2020 and 2021, the list of luxury hotel chains, booking sites, and retailers that now accept cryptocurrency has continued to grow. *See* Emily Nicolle, *It's Not Just Tesla That Takes Bitcoin—These Shops Will Take Your Payment in Crypto Too,* FIN. NEWS LONDON (Mar. 12, 2021), https://www.fnlondon.com/articles/its-not-just-tesla-that-takes-bitcoin-heres-a-list-of-retailers-accepting-payment-in-crypto-20210312 (explaining that Tesla, Apple, and Spotify are among the retailers that now accept cryptocurrency).

broker), or schedule an in-person meet up to conduct a transaction. According to a Cornerstone Advisors study cited by Forbes, as of July 2020, 15% of American adults owned some form of cryptocurrency.[74] According to the study, that percentage drastically increased from March to July of 2020 during the first few months of the pandemic, with many of the owners purchasing it for the first time in 2020.[75] Nearly one year later, the percentage was even higher. In May of 2021, a New York Digital Investment Group study found that 17% of adult Americans now own some amount of Bitcoin.[76] The United States now ranks in the top 10 for cryptocurrency consumers.[77]

Using cryptocurrency is not inherently illegal. The decentralized nature of cryptocurrency, the ease of conducting transactions, and the



[74] Ron Shevlin, *The Coronavirus Cryptocurrency Craze: Who's Behind the Bitcoin Buying Binge*, FORBES (July 27, 2020), https://www.forbes.com/sites/ronshevlin/2020/07/27/the-coronavirus-cryptocurrency-craze-whos-behind-the-bitcoin-buying-binge/?sh=44423eb92abf; *see* Spencer Bogart, *Bitcoin is a Demographic Mega-Trend: Data Analysis*, Blockchain Cap. Blog (Apr. 30, 2019), https://medium.com/blockchain-capital-blog/bitcoin-is-a-demographic-mega-trend-data-analysis-160d2f7731e5 (citing study estimating 9% of U.S. consumers owned bitcoin in early 2019 and 18% of consumers age 18–34).
[75] Shevlin, *supra* at 74.
[76] *46 Million Americans Now Own Bitcoin*, NASDAQ (May 14, 2021), https://www.nasdaq.com/articles/about-46-million-americans-now-own-bitcoin-2021-05-14.
[77] *Id.*; Connor Sephton, *Revealed: The Countries With the Highest Levels of Every Day Crypto Use*, MOD, CONSENSUS (Sept. 9, 2020), https://modernconsensus.com/cryptocurrencies/bitcoin/revealed-the-countries-with-the-highest-levels-of-everyday-crypto-use/ (citing Chainalysis' 2020 Global Crypto Adoption Index).

global nature of its use, however, make it a prime tool for criminals.[78] Instead of heading to the bank, where there may be video surveillance and an identification requirement to conduct a transaction, offenders can conduct multiple different transactions—which do not require them to provide a name or address—within seconds, without ever leaving their home. Moreover, they can easily transact with people in multiple other countries.

Because human trafficking is so lucrative and often requires moving around large amounts of money, cryptocurrency is increasingly used to facilitate it.[79] Furthermore, in many cases, credit card companies now refuse to process transactions for websites that are suspected of facilitating sex trafficking. Traffickers and their customers have turned to cryptocurrency as a successful workaround. For example, in the summer of 2015, as criticism mounted against Backpage, both Visa and MasterCard refused to process Backpage-related transactions. Backpage turned to Bitcoin as an alternative, offering a 10% discount to anyone who used it to post ads.[80] Because nearly all cryptocurrency is decentralized, there is no decisionmaker who can remove it from the sex trafficking equation, regardless of the political climate. Cryptocurrency allows individuals to easily conduct transactions completely outside of regulated financial and payment systems.

In some cases, focusing on the use of cryptocurrency may be a starting point for an investigation. In others, it can corroborate and help identify co-conspirators, witnesses, and victims. If an offender's

---

[78] *See* Brett Nigh & C., Aiden Pelker, *Virtual Currency: Investigative Challenges and Opportunities*, FBI L. ENF'T BULL. (Sept. 8, 2015), https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities.

[79] *See, e.g.,* Brett Israel, *In a Step Toward Fighting Human Trafficking, Sex Ads are Linked to Bitcoin Data*, BERKELEY NEWS (Aug. 16, 2017), https://news.berkeley.edu/2017/08/16/in-a-step-toward-fighting-human-trafficking-sex-ads-are-linked-to-bitcoin-data/.

[80] Sasha Aslanian, *For Sex Industry, Bitcoin Steps In Where Credit Cards Fear to Tread*, NAT'L PUB. RADIO (Dec. 15, 2015), https://www.npr.org/sections/alltechconsidered/2015/12/15/456786212/for-sex-industry-bitcoin-steps-in-where-credit-cards-fear-to-tread; Jessica Hoyer, *Sex Trafficking in the Digital Age: The Role of Virtual Currency-Specific Legislation in Keeping Pace with Technology*, 63 WAYNE L. REV. 83, 103–04 (2017).

use of cryptocurrency is traceable, it can be seized, forfeited, and when appropriate, used to compensate victims.

So, how does one begin to investigate cryptocurrency when it poses the challenges discussed above? Although cryptocurrency does provide anonymity in some ways, for most cryptocurrencies, that anonymity is limited. For example, Bitcoin users maintain the entire transaction history for the virtual currency to prevent users from double spending, that is, transferring the same bitcoin twice.[81] Each transaction is time-stamped and grouped in blocks, and each block references the prior block.[82] The *blockchain*, or the entire transaction history of Bitcoin, is publicly accessible.[83] Although the blockchain itself does not contain information identifying virtual currency users, it provides the amounts exchanged, the date and time of the transactions, and the addresses relating to the transactions—data points that can help identify the target.[84] For example, if the target used an exchange, the blockchain may show which exchange, and law enforcement can potentially subpoena the exchange for identifying information.[85]

Moreover, a number of private companies now specialize in analyzing blockchain data to identify users. These companies have created investigative tools that are available to law enforcement. Examples of these companies include Chainalysis, Coinbase Analytics, CipherTrace, and Elliptic,[86] with several more just emerging.

---

[81] Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, IMC 2013—Proceedings of the 13th ACM Internet Measurement Conference, U.C. SAN DIEGO & GEO. MASON U. 1–2 (2013).
[82] *Id.* at 2.
[83] *Id.*
[84] Addresses are identifiers that represent the possible destination or origin of a cryptocurrency transaction.
[85] Exchanges are subject to legal process and typically must meet some degree of "Know Your Customer" (KYC) requirements. Matthew Cronin, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*, 66 U.S. ATTY'S BULL., no. 4, 2018, at 65, 68. These vary depending on their host country. *Id.* They can include the target's actual name, date of birth, associated email, IP information, other services used, phone numbers, and even bank information. *See* Korver et al., *supra* note 68, at 249.
[86] Danny Nelson, *Coinbase Offers US Feds New Crypto Surveillance Tools*, COINDESK (June 5, 2020), https://www.coindesk.com/coinbase-analytics-blockchain-analysis-crypto-government.

Many of these companies specifically recognized the increasing use of cryptocurrency to facilitate human trafficking. For example, in February 2020, CipherTrace published an article entitled *Fighting Human Trafficking by Following the Money*, detailing its efforts to trace cryptocurrency and its partnership with the Anti-Human Trafficking Intelligence Initiative.[87] Chainalysis also published an article entitled, *Making Cryptocurrency a Part of the Solution to Human Trafficking*, noting the thousands of human trafficking-related SARs filed in 2018 and positing that, in the wake of FOSTA and because child pornography is often linked to sex trafficking, traffickers are increasingly turning to cryptocurrency.[88]

Some of these companies' tools have been successfully used to facilitate federal investigations. Prosecutors should consult the Money Laundering and Asset Recovery Section (MLARS) before engaging with a specific company. There are also a number of free resources (some provided by commercial companies) on blockchain analysis, including tools that enable users to search for transaction history relating to a specific address.[89] These may be helpful tools for prosecutors and law enforcement to better understand how to analyze a blockchain in their particular case.

Aside from blockchain analysis, there are several other potential sources of information when it comes to proactively investigating human trafficking based on the use of cryptocurrency. First, administrators and exchangers of virtual currency are MSBs under applicable regulations and must comply with the FinCEN registration and reporting requirements described above.[90] Investigators can

---

[87] Pamela Clegg, *Fighting Human Trafficking by Following the Money*, CIPHERTRACE (Feb. 1, 2020), https://ciphertrace.com/fighting-human-trafficking-by-following-the-money/.

[88] *Making Cryptocurrency Part of the Solution to Human Trafficking*, CHAINALYSIS (Apr. 21, 2020), https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020.

[89] *See* Korver et al., *supra* note 68, at 248.

[90] 76 C.F.R. § 43585-01; Press Release, Fin. Crimes Enf't Network, FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities (Mar. 18, 2013). In addition, in January 2021 the National Defense Authorization Act for Fiscal Year 2021 (NDAA) was passed wherein Section 6102 brings virtual currency within the scope of the definitions of "financial institution," "monetary transaction," "money transmitting business," and "money transmitting service" under the BSA.

therefore search for SARs filed by virtual currency exchanges that relate to the use of cryptocurrency and use key words indicative of human trafficking. Second, virtual currency transactions must be reported to the IRS, and tax returns may therefore provide useful information.[91]

Third, other government organizations, including the Securities and Exchange Commission and the Commodity Futures Trading Commission (CFTC),[92] regulate cryptocurrency, and numerous states have enacted cryptocurrency regulations as well.[93] The nature and extent of these regulations is ever changing. For example, in the 116th Congress, the House considered the "Crypto-Currency Act of 2020," which would have changed the regulatory scheme with respect to "digital assets," as defined in the bill.[94] A visual of state regulation as of September 23, 2020, is depicted below:[95]

---

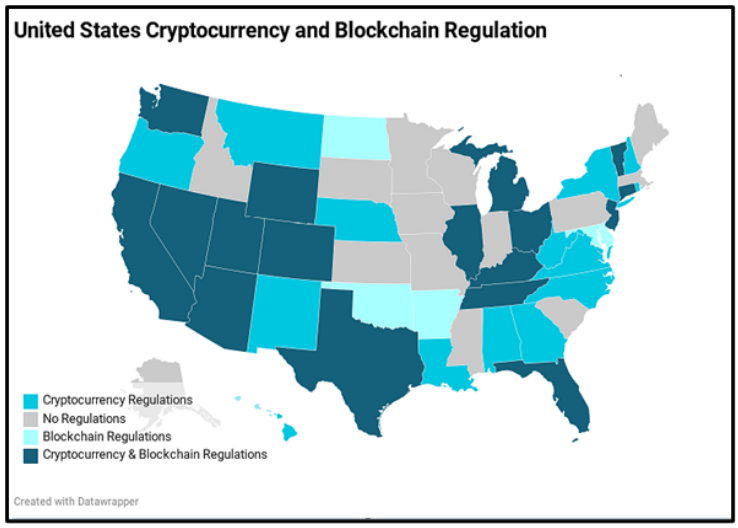
[91] Virtual Currency is considered property.

[92] *See* Korver et al., *supra* note 68, at 243.

[93] Shelagh Dolan, *How the Laws & Regulations Affecting Blockchain Technology and Cryptocurrencies, Like Bitcoin, Can Impact its Adoption*, BUS. INSIDER (Mar. 3, 2020), https://www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global.

[94] *See* H.R. 6154, 116th Cong. (2020) (introduced but not passed).

[95] The above map was created after surveying a number of resources, including state legislation and regulations. *See, e.g.,* Matthew Kohen, et al., *State Regulations on Virtual Currency and Blockchain Technologies* (July 14, 2020), https://www.jdsupra.com/legalnews/state-regulations-on-virtual-currency-66988/; *see also* Heather Morton, *Cryptocurrency 2021 Legislation*, Nat'l Conf. of State Legislatures (Mar. 22, 2021), https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2021-legislation.aspx (summarizing 2021 state legislation).



Once a human trafficking target using cryptocurrency is identified, there are many things to consider. First, each agency has a cryptocurrency seizure policy. Before entering a residence, agents should know what this policy is and be prepared to implement it. Moreover, agents with a background and understanding of cryptocurrency and dark-web applications should be a part of any search, any forensic preview or examination of devices, and the interview of any target.

Second, the entire search team should be aware of the different ways in which private keys may be stored, and the search warrant and attachments should include these locations. The search team should also be aware of what private keys look like—typically a string of characters. They can be handwritten, printed, in a Word document or other digital document, in the form of a QR code, in a wallet client, saved in an application on a smart phone, or hidden in a secure place. If cryptocurrency is discovered during a search, agents should transfer it to an agency-controlled wallet and hold it on a secure device that is not connected to the internet.[96]

As in other complex cases involving multiple criminal actors, targets who use cryptocurrency will often know the identity of, or have information that can help lead to the identification of, other more sophisticated targets. They may even be able to facilitate undercover work that may prove to be the sole way of identifying other co-

[96] *See* Korver et al., *supra* note 68, at 257.

conspirators. If an arrest is made, prosecutors may want to seek to have defendants detained so they do not warn confederates or access and move funds that are not yet seized. Prosecutors should take extra care not to identify sensitive law enforcement techniques in public filings by sealing documents and obtaining protective orders. Prosecutors should also keep in mind that exchanges and others involved in the cryptocurrency market value privacy and may disclose legal process whether permitted to or not.[97]

The existence of cryptocurrency has often been mentioned only in passing or appeared as a footnote in prosecutions involving human trafficking. However, as those involved in the online advertisement of commercial sex are subject to more scrutiny in the wake of Backpage's shutdown and the enactment of FOSTA, and as cryptocurrency becomes more fungible, the use of cryptocurrency will no longer be just an afterthought in human trafficking investigations.

V. Conclusion

In the last three years, new legislation, the shutdown of several websites facilitating and profiting from sex trafficking, and technological advancements—including the increased use of cryptocurrency—have forever altered how human traffickers use the internet to facilitate their crimes. As offenders adapt to these changing circumstances, so must law enforcement. Prosecutors have perhaps more tools and partners than ever before to proactively investigate sex trafficking. But we must leverage those tools by understanding the new world of online commercial sex and coordinate with our partners in both the private sector and state law enforcement.

About the Authors

Jane Khodarkovsky is a Trial Attorney in the Money Laundering and Asset Recovery Section (MLARS), Criminal Division. She investigates and prosecutes multi-jurisdictional and international

---

[97] There are other useful resources for prosecutors conducting these investigations that, while not focused on human trafficking, dive far deeper into the world of cryptocurrency. These include Matthew Cronin's article "*Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*," *supra* note 85, and "*Attribution in Cryptocurrency Cases*," by Michele Korver, C. Alden Pelker, and Elisabeth Poteat, *supra* note 68.

money laundering and financial crimes. She also serves as a subject-matter expert on how to conduct money laundering investigations in human trafficking and child exploitation cases for U.S. Department of Justice (Department) components; U.S. Attorney's Offices; and federal, state, and local law enforcement. She regularly provides guidance and training on forfeiture and restitution for victims of human trafficking. Before joining the Department, she prosecuted enterprise corruption, scheme to defraud, larceny, public corruption, and tax fraud schemes often involving money laundering at the New York County District Attorney's Office and the New Jersey Attorney General's Office. She graduated from the University of Michigan Law School, where she represented victims in the Human Trafficking Clinic and served as Executive Editor of the Michigan Journal of Race and Law, and clerked for the Hon. Ronald D. Wigler, P.Cr. in New Jersey.

April Nicole Russo is a Senior Assistant United States Attorney in the Child Exploitation and Human Trafficking Section of the U.S. Attorney's Office for the District of Columbia and serves as the district's Project Safe Childhood Coordinator. Before joining the D.C. U.S. Attorney's Office, she worked as an Assistant United States Attorney (AUSA) in the Eastern District of Michigan for over five years, where she earned the distinction of the role of Deputy Chief of the Major Crimes Unit and served as the district's Project Safe Childhood and Human Trafficking Coordinator. As an AUSA, she has prosecuted a wide variety of cases, including sex trafficking, aggravated sexual abuse, violations of the Mann Act, production of child pornography, child exploitation enterprise involving four different international child pornography rings, kidnapping, carjacking, and distribution-causing-death. April has presented on child exploitation at a number of national and international conferences, to include Canada's Multidisciplinary Training Conference to Protect Children from Sexual Abuse, the BOLT Conference, the National Law Enforcement Training on Child Exploitation, and the AHRC's Community Forum on Human Trafficking. Before becoming an AUSA, she worked as an Assistant District Attorney in Philadelphia. After graduating from the University of Virginia Law School in 2011, April clerked for Federal District Judge Robert E. Payne before becoming a prosecutor.

Lauren E. Britsch is a former Trial Attorney in the Criminal Division's Child Exploitation & Obscenity Section, where she

prosecuted cases involving child sex trafficking, online child exploitation, child sexual abuse, production of child pornography, and international child sex tourism in federal district courts around the country. She was also a Special Assistant United States Attorney in the Cybercrime Unit in the Eastern District of Virginia. Lauren has presented on topics related to sex trafficking and child exploitation at international trainings in Cambodia and the Bahamas, as well as at the annual Internet Crimes Against Children conferences in Seattle and Atlanta. For her work at CEOS, Lauren received multiple Assistant Attorney General's Awards, including the 2018 Award for Outstanding Contributions by a New Employee. She graduated from Georgetown University Law Center in 2013 and clerked for District Judge Daniel P. Jordan III in the Southern District of Mississippi. She is now a Trial Attorney in the Public Integrity Section of the Criminal Division.

Surfing the First Wave of Cryptocurrency Money Laundering

Alexandra D. Comolli
Management and Program Analyst
Money Laundering, Forfeiture, and Bank Fraud Unit
Federal Bureau of Investigation

Michele R. Korver
Digital Currency Counsel
Criminal Division
Money Laundering and Asset Recovery Section

"You can't stop the waves, but you can learn to surf."[1]

I. Introduction: a revolution—and a gnarly wave—unleashed

Bitcoin was unveiled to the world in January 2009. Its pseudonymous creator, Satoshi Nakamoto, pieced together this creation with cryptography, systems engineering, and economics.[2] He, she, or they designed a self-sustaining distributed system that would allow individuals to exchange value without a centralized arbiter. In other words, an internet of value. Nakamoto's vision is now reality. Value can be transferred around the world, *ad infinitum*, without ever touching a financial institution. While this is likely a revolutionary technology, it also created new money laundering risks.

For practitioners working in areas that touch upon cryptocurrency, this article describes what the first wave of cryptocurrency money laundering looks like, discusses what regulations and laws apply to such conduct, and touches on some emerging business models and techniques that will likely drive the second and third waves of cryptocurrency money laundering.

---

[1] JON KABAT-ZINN, WHEREVER YOU GO, THERE YOU ARE: MINDFULNESS MEDITATION IN EVERYDAY LIFE (2005).
[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Oct. 2008.

As described below, cryptocurrency-related money laundering has followed the traditional placement, layering, and integration model, but it does so with a new set of technologies and gatekeepers.

II. Why cryptocurrency is a unique money laundering tool

The history of Bitcoin and other cryptocurrencies has been thoroughly covered in academic literature and, therefore, is not covered here. For the purposes of this article, the following features of cryptocurrencies—and their underlying blockchains—are most important:

- They are decentralized;
- they are pseudonymous;
- they are immutable; and
- their ledgers may be transparent or opaque.

But before delving into these features, we need a primary definition. Cryptocurrency, a type of virtual currency, is a decentralized peer-to-peer network-based medium of value or exchange. Cryptocurrency may be used as a substitute for government-backed "fiat" currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[3] Early virtual currencies, like E-Gold, facilitated substantial money laundering, but for the reasons explained below, did not create a new paradigm for transferring value. Rather, they were centralized and depended on an institution to clear transactions. Accordingly, when those institutions broke bad, they were shut down like any other dirty financial institution. As explained below, cryptocurrency is a paradigm shift that permanently changed the money laundering landscape.

A. Decentralized

Cryptocurrencies are decentralized in that the processing and confirmation of transactions takes place through users and not through a centralized authority, such as a bank.[4] In avoiding a centralized authority, cryptocurrencies can, at least in theory, allow

[3] Michele R. Korver et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233.

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (n.d.).

individuals to move funds without interacting with a regulated gatekeeper, such as a depository institution or a money services business. Accordingly, in the traditional typology of money laundering, cryptocurrencies allow criminals to breeze through the placement and layering stages, though as described below, the integration stage remains a major obstacle—largely because cryptocurrency is not yet a widely adopted means of payment for goods and services.[5]

Decentralization also means that there may not be a centralized institution to prosecute if a cryptocurrency is used for illegal purposes. Even though individuals and coding committees are responsible for continually updating a cryptocurrency's code, that body usually is not responsible for confirming individual transactions and, thus, is not in the same position as, for instance, the principals of E-Gold. The lines may become more blurred, however, in the context of decentralized exchanges, where the purpose of the software is to facilitate money transmission, and the owners of such software make a commission on those transactions.

B. Pseudonymous

Pseudonymity is the partially anonymous state in which a user maintains consistent identifiers—in this case, wallet addresses—that are different from the user's official identifiers, such as a name and social security number. For a cryptocurrency blockchain to confirm transactions, it must be able to verify inputs and outputs to and from wallet addresses. 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. Nonetheless, even with this risk, cryptocurrencies allow criminals to digitally transact without providing standard identification

---

[5] CHAINALYSIS, THE 2020 STATE OF CRYPTO CRIME 7 (Jan. 2020) ("Money laundering is the common denominator between all forms of crypto crime, because every criminal earning cryptocurrency illegally eventually needs to obscure the origins of their holdings in order to convert them to cash.").

information to a regulated gatekeeper—much like individuals exchanging cash in-person.

C. Transparent

Closely related to pseudonymity is whether a blockchain is transparent. This feature is often confused with the public/private distinction, but it is in fact different. A blockchain can be any combination of these four features. The public/private feature of a blockchain refers to who has permission to use it. In other words, a public blockchain is one that anyone can transact in and, thus, does not require special permissions, whereas a private blockchain limits access to specific users (and is often used by a single company or conglomeration). Conversely, the transparency of a blockchain refers to who can observe it.

In the context of cryptocurrency, a transparent blockchain, such as the Bitcoin blockchain, allows the public to see the entire history of every transaction ever conducted on it. By contrast, an opaque blockchain, such as the types employed by so-called anonymity or privacy-enhanced coins, prevent the public from seeing the source, amount, or destination of any transaction. Transparent blockchains hold two main advantages: First, they often operate more efficiently because transactions carry less technical layers of obfuscation technology, and second, they are more easily adaptable for applications beyond cryptocurrency. A third and more speculative benefit is that transparent blockchains lack the risk factors associated with privacy coins that either overtly or functionally cater to the criminal element. A combination of these three factors is likely the reason why privacy coins are less widely used.[6]

In the context of money laundering, opaque blockchains are more problematic. As noted above, transparent blockchains allow law enforcement to connect the dots between transactions. If Jane Doe is found to be the user of wallet *Z*, then in theory, the entire history of the inputs into that wallet can be discovered—not so on opaque blockchains. Monero, for example, uses *ring signatures* that mix inputs to obscure their historical trails. Yet, it appears unlikely that the technology underpinning privacy coins will win the arms race

[6] *Privacy* C*oins*, CRYPTOSLATE, https://cryptoslate.com/cryptos/privacy/ (last visited May 10, 2021).

against crypto-investigative companies.[7] Even so, opaque blockchains will continue to add another layer of frustration to those attempting to trace cryptocurrency transactions.

D. Immutable

Blockchains are immutable because the verification of present time transaction *Z* depends on its historical antecedents. In other words, you cannot confirm a transaction if it does not correspond to all prior transactions in its history. The immutability of blockchains is what makes them a likely source of highly useful applications unrelated to cryptocurrency. In more concrete terms, a block in a blockchain is equivalent to a photo of someone holding up the front page of the *New York Times*, which reveals that the photo could not have been taken on a later date than what is printed on the paper. But unlike a photo, which can be doctored, each transaction on a blockchain has a unique hash, which proves it is the legitimate successor to all previous transactions on the blockchain.[8] Any change to the content of those transactions results in a different, illegitimate hash.

Useful applications can be built into blockchains because of this feature, including smart contracts, identity verification, and restricted data storage. For law enforcement, the immutability of blockchains is advantageous. The immutability of blockchains means that the data contained in them is tamper-proof. As such, if a criminal can be tied to transactions on a blockchain, she cannot claim that they were fake. Relatedly, blockchains are easy to authenticate at trial, even without a custodian of records. While prosecutors may choose to call a subject-matter expert to explain how blockchains work and to present the specific transactions at issue, the data itself doesn't need further authentication because it is confirmed by the system itself. In sum,

---

[7] Rachel Wolfson, *CipherTrace Develops Monero Tracing Tool to Aid US DHS Investigations*, COINTELEGRAPH (Aug. 31, 2020), https://cointelegraph.com/news/ciphertrace-develops-monero-tracing-tool-to-aid-us-dhs-investigations.

[8] "A transaction hash/id is a unique string of characters that is given to every transaction that is verified and added to the blockchain. In many cases, a transaction hash is needed in order to locate funds." *What is a Transaction Hash/Hash ID*, COINBASE, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/what-is-a-transaction-hash-hash-id#:~:text=A%20transaction%20hash%2Fid%20is,in%20order%20to%20locate%20funds (last visited May 10, 2021).

immutability is a feature of blockchains that benefits law enforcement and the accused, if using blockchain evidence as a defense.

III. Money laundering 101: placement, layering, and integration

Rather than abstractly defining money laundering, it makes more sense to describe the purpose it serves. At its core, money laundering is about making dirty money usable. "Money-laundering . . . [is] the process of trying to disguise illicit-profits in order to enjoy the use of all ascribed legitimate, standardised and commonly shared agentive functions of money while the criminal origins of the entity incorporating these functions (*money*) are hidden."[9] The process of money laundering is traditionally divided into three stages: placement, layering, and integration (PLI). This schema makes sense but rarely applies neatly to any specific money laundering scheme.

Briefly, placement is getting the dirty proceeds into or through a gatekeeping institution, such as a bank, money services business (MSB), or informal value transfer system (such as hawala).[10] Once placed into one of these institutions, a criminal can begin carrying out transactions to obscure the source, nature, ownership, or control of the proceeds.[11] Layering can involve wire transfers, ACHs,[12] person-to-person handoffs, and in the context of cryptocurrency,

---

[9] Dionysios S. Demetis, A Systems Theoretical Approach for Anti-Money Laundering Informed by a Case Study in a Greek Financial Institution 19 (Jan. 2008) (Ph.D dissertation, London School of Economics and Political Science) (ProQuest).

[10] "Hawala is an alternative or parallel remittance system. It exists and operates outside of, or parallel to traditional banking or financial channels. It was developed in India, before the introduction of Western banking practices, and is currently a major remittance system used around the world. . . . Hawala works by transferring money without actually moving it." PATRICK M JOST, U.S. DEP'T OF THE TREASURY & HARJIT SINGH SANDHU, INTERPOL, THE HAWALA ALTERNATIVE REMITTANCE SYSTEM AND ITS ROLE IN MONEY LAUNDERING (n.d.).

[11] 18 U.S.C. § 1956 (a)(1)(B)(i).

[12] Automated Clearing House, or ACH, "transfers are a way to move money between accounts at different banks electronically." Rebecca Lake, *ACH Transfers: What Are They and How Do They Work*, INVESTOPEDIA (Apr. 30, 2021), https://www.investopedia.com/ach-transfers-what-are-they-and-how-do-they-work-4590120.

movement of funds from various wallet addresses (often done through mixing and tumbling services). The final broad stage of money laundering is integration, in which the proceeds are blended into the criminal's existing life to make them potentially undetectable. For example, placement occurs when a criminal takes laundered funds out of *front accounts* to purchase luxury items like vehicles and real property. Once purchased, the vehicles and real property can be described as *integrated* into the criminal's financial holdings, thus completing the PLI cycle.

Different money laundering techniques are associated with different parts of the PLI process. For example, structuring, in which a criminal manipulates cash deposits to prevent a gatekeeper from filing a mandated report—such as a Currency Transaction Report or (CTR)—is typically part of the placement stage. Likewise, intricate conversions of proceeds to other forms of value, such as from cash to electronic funds to precious metals and back to cash, are part of the layering phase. As described in detail below, cryptocurrency money laundering often follows the PLI model, but sometimes at a faster pace, particularly in the layering phase. This is largely because of the decentralized nature of cryptocurrency, which allows transactions to be made quickly and globally without using a trusted third party that would be obligated to carry out due diligence on customers and transactions.[13]

Before examining how cryptocurrency money laundering looks through the prism of the PLI model, it is helpful to first understand the most common crimes involving cryptocurrency.[14] As described in more detail below, the typical flow of funds in cryptocurrency money laundering is from cryptocurrency to fiat currency.[15] This movement

---

[13] Demetis, *supra* note 9, at 25 ("[Cyber-laundering] magnifies the problem because of two interconnected reasons: the first is that the laundering phases may be carried out more easily, and the second is because dematerialized e-cash and its subsequent liquidity provide the opportunity for disintermediation, bringing the buyer and the seller in a direct relationship.").

[14] *Id.* at 19 ("[A]ny definition on money laundering must also encompass the nature of the money being laundered, with reference to the functionality that it serves.").

[15] Fiat money is currency that lacks intrinsic value and is established as a legal tender by government regulation. *Fiat*, OXFORD ENG. DICTIONARY,

occurs because criminals may obtain ill-gotten funds in the form of cryptocurrency and need to make it usable by converting it to fiat currency and other tangible assets. Dark web commerce illustrates how the flow of funds move from cryptocurrency to fiat currency. In this ecosystem, vendors of illegal goods and services are paid in cryptocurrency because no institutional payment processors, such as Visa or Mastercard, will allow their services to be used on dark web marketplaces. Vendors of narcotics, hacking tools, stolen personally identifiable information, and illegal services often end up with bulks of cryptocurrency that need to be converted into fiat currency, which can be used to buy tangible goods or reinvested into an illegal enterprise.

The same flow of funds from cryptocurrency to fiat currency appears outside of dark web commerce. For example, ransomware attackers almost always collect their payments in cryptocurrency. They do this for many reasons, including the certainty and transparency of the payment method and the ability to quickly layer the victim's funds. The same flow of funds occurs when an institutional exchange is hacked. The attackers gain huge sums of cryptocurrency, which must be laundered and converted into fiat currency.

None of this is to say that crypto-laundering doesn't also take place in the reverse. It's possible to imagine tax cheats converting their income into cryptocurrency and then keeping the funds in that form to attempt to avoid scrutiny from tax authorities. In addition, fraudsters are increasingly converting victim funds collected in fiat to cryptocurrency to conceal the funds and attribution evidence from law enforcement, as well as to quickly and easily move the proceeds from one jurisdiction to another.[16] Similarly, transnational criminal organizations may use P2P exchangers and other third party money launderers to convert cash proceeds of crime to cryptocurrency in order to efficiently move the funds among co-conspirators or across international borders.[17]

With this in mind, we can first look at the *placement* of cryptocurrency. In one sense, placement is almost risk-free, just like

---

https://www.oed.com/view/Entry/69729?redirectedFrom=fiat+money#eid4394015 (last visited Feb. 18, 2021).

[16] *See, e.g.,* Press Release, U.S. Dep't of Justice, Owner of Bitcoin Exchange Convicted of Racketeering Conspiracy for Laundering Millions of Dollars in International Cyber Fraud Scheme (Sept. 28, 2020).

[17] *See, e.g.,* CHAINALYSIS, THE 2021 CRYPTO CRIME REPORT 23–24 (Feb. 2021).

when someone puts cash in a billfold. Because cryptocurrency wallets can be set up without a third-party, criminals can put funds into those wallets without any oversight. But even if wallets can be easily funded, at some point the criminal may have to place those funds into an account controlled by a regulated gatekeeper. For example, if a criminal wants to use a regulated cryptocurrency exchange, the placement of dirty crypto funds may carry the same risk as a criminal placing dirty cash into a bank. Indeed, data on cryptocurrency crime suggests that most criminal proceeds are laundered through regulated gatekeepers.[18] If operated in a compliant manner, the cryptocurrency exchange will obtain "Know Your Customer" (KYC) information, make risk assessments, and file federally mandated reports.[19] The criminal may circumvent this step by going through a non-compliant cryptocurrency exchange. As discussed below, regulation and enforcement has been slow to catch up with illegally operated exchanges, leaving room for criminals to easily launder their funds. Nonetheless, this advantage is temporary as cryptocurrency exchanges and service providers worldwide are increasingly being regulated to the same extent as traditional financial institutions. As such, the initial placement (of cryptocurrency into a wallet) is entirely different in the context of cryptocurrency, but the more significant step of using an intermediary entity that can actually convert the cryptocurrency into fiat currency, and vice versa, isn't much different than in the fiat world.

The second stage of *layering* is where criminals can take creative measures with cryptocurrency—with the risk that every transaction creates a trail that can later be traced back to them. Not having to use a third-party to conduct transactions, criminals can layer their funds by simply setting up multiple cryptocurrency addresses and having the funds sent through those addresses. This movement, sometimes called *tumbling*, can make it difficult to track the historical flow of funds (though the advancement of blockchain analytics has made this type of layering much less effective for criminals). Instead of sending the funds from Point *A* to Point *B*, the funds are sent through intermediary wallets for the sole purpose of creating distance from the

---

[18] *Id.* at 9–10.

[19] KYC refers to a set of standards used within the investment and financial services industry to verify customer identities, their risk profiles, and financial profiles. *See, e.g.,* 31 C.F.R. § 1022.210.

original point of entry.[20] These transactions likely occur without touching a regulated gatekeeper, and thus, no mandated reports such as Suspicious Activity Reports (SAR) are filed.[21] Some may think of this as a digital hawala, but it is different in that a blockchain itself is not a regulated entity, unlike a hawala—which would be required to register as a money transmitting business and also file mandated reports with the Financial Crimes Enforcement Network (FinCEN). At the same time, every additional wallet used by a criminal is an additional breadcrumb that law enforcement can use to connect the dots of that criminal's historical conduct. Along these same lines, blockchains can also remove geographic barriers to moving funds. The possession of funds on a blockchain is based on control of a wallet's private keys.[22] Thus, a criminal can transfer ownership simply by providing the private keys to someone else, all without ever touching a financial gatekeeper. Similarly, instead of transferring the private keys, criminals can send the value to other wallet addresses.

A wallet does not exist in a specific physical place but is, instead, just software that interacts with a blockchain. The location of the wallet is wherever control of the private keys is located. Maybe that is the location of the IP address used by the owner when trying to access the value, or maybe, in the case of cold storage wallets, it is wherever the container of the private keys is located. Just as the internet extracted information from the kinetic world, blockchains have done the same for value. The key point is that the location of the funds can be both everywhere and nowhere at the same time.

By comparison, it is useful to think through the many steps a traditional drug trafficking organization (DTO) must go through to

---

[20] *See* U.S. DEP'T OF JUST., CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 41 (Oct. 2020) [hereinafter CRYPTOCURRENCY ENFORCEMENT FRAMEWORK]. Similar to tumbling, *mixing* may also be part of the money laundering strategy at this stage, but because mixing services may be regulated entities, they are discussed later in the paper.

[21] *See* 31 U.S.C. § 5318(g).

[22] A private key is a cryptographic code that allows users to access their cryptocurrency while ensuring that users' funds are protected from theft and unauthorized access.

physically move the proceeds of its endeavors from the location of distribution back to the location of manufacturing. Sometimes, DTOs use funnel accounts to geographically move funds, that is, *smurfs* for the DTO deposit cash at bank branches in one region and have it withdrawn in another. This is a time-consuming and risky process because financial institutions may file SARs or CTRs on the transactions—or maybe the smurfs are unreliable and steal a portion of the funds, say something stupid to the bank teller when making a transaction, or the bank closes the accounts for suspicious activity. To avoid all of this, DTOs could require their customers, or at least their lower level distributors, to pay in cryptocurrency. The funds could then be immediately transferred from one region to another, without ever touching a regulated institution. At some point, the DTO will have to convert the funds to fiat currency or some other usable form of value (the integration stage of the money laundering process), but that is a different problem for the DTO. By accepting cryptocurrency, it can potentially eliminate one of its primary money laundering concerns (though, as noted before, these transactions are still recorded on a blockchain, which leaves historical traces of all transactions for law enforcement to later analyze).

This is not to say that the placement and layering stages do not pose any risk to criminals. Several blockchain analytics companies dedicate significant resources to mapping the major blockchains. This allows users of these analytic platforms to see if funds are moving to or from illicit sources, such as wallets associated with dark web marketplaces. In theory, funds coming from dark web marketplaces could be traced to a regulated gatekeeper, such as a cryptocurrency exchange or mixing service, where law enforcement could then simply issue a subpoena for account records to the institution and work backwards from that identifying information. In other words, the mere movement of funds from an identified illicit source can pose some risk to criminals.

While cryptocurrency may provide some new money laundering techniques at the placement and layering stages, it has yet to make any changes to the traditional problems associated with integration. The key word is *yet*—cryptocurrency is still largely unusable at a consumer level, which means criminals must convert it to a usable

form, such as fiat currency.[23] Criminals often first encounter regulated gatekeepers at the point of conversion. They may go to a peer-to-peer (P2P) or institutional exchanger to cash out their ill-gotten cryptocurrency, but these individuals and institutions are subject to the Bank Secrecy Act and are required to maintain an anti-money laundering program and file SARs and CTRs. As discussed below, some exchangers base their business model on violating these regulations and, unsurprisingly, can charge premiums to criminals who would otherwise be screened out by compliant exchangers. Many of the crooked exchangers, however, get caught, and when this happens, their customers are discovered, as was the case with Operation Dark Gold, which is discussed below. The risks are thus unavoidable when the criminal attempts to convert her cryptocurrency to fiat. As such, until cryptocurrency becomes widely accepted at a consumer level, criminals will still be forced to integrate those funds into fiat currency, where they will encounter higher levels of risk than in the placement and layering stages.

In sum, crypto money laundering follows the general PLI model but offers some new money laundering techniques (though also with some new risks for criminals) with these new techniques. Even with the great money laundering advantages created by cryptocurrency, criminals still must convert those funds to something more usable in the fiat world. To do so, they generally must use a regulated gatekeeper. It is at this stage where any advantage for criminals is lost.

IV. The primary domains of cryptocurrency money laundering

Criminals follow common paths when placing, layering, and integrating their ill-gotten cryptocurrency. Those paths go through several primary domains, including institutional exchanges, P2P

---

[23] There are, however, many companies and retailers who accept bitcoin and other cryptocurrencies such as websites for postage, Microsoft, AT&T, some fast food restaurants, Overstock, airlines (Virgin and Norwegian Air), professional sport teams, and various online game and clothing sites, just to name a few. Ofir Beigle, *Who Accepts Bitcoin as Payment?*, 99BITCOINS (Jan. 7, 2021), https://99bitcoins.com/bitcoin/who-accepts/; Jordan Tuwiner, *Who Accepts Bitcoint? 11 Major Companies*, BUY BITCOIN WORLDWIDE (Apr. 28, 2021), https://www.buybitcoinworldwide.com/who-accepts-bitcoin/.

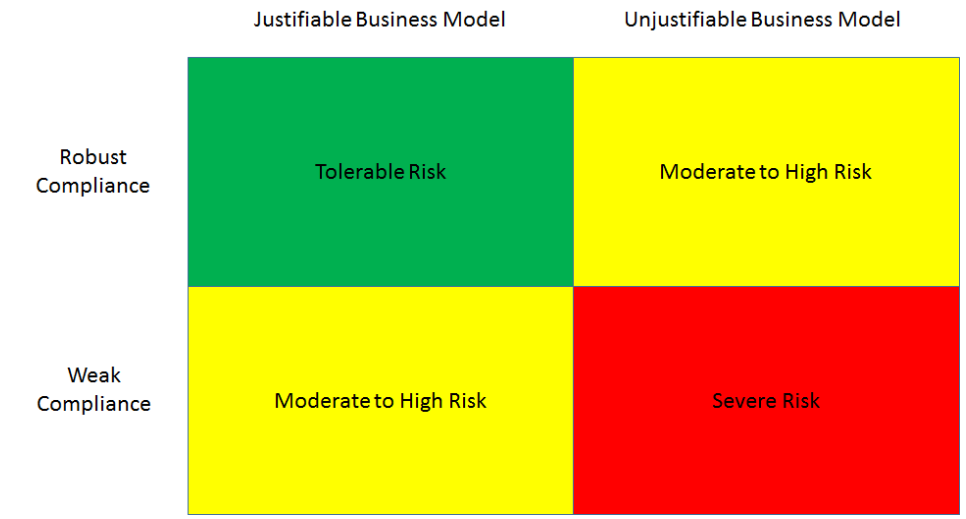
exchangers, mixing and tumbling services, and traditional banks. These paths aren't static, and it should be expected that certain emerging technologies, such as decentralized exchanges, will become a primary domain in the near future.[24] Some of these primary domains, such as P2P exchangers and mixing services, appear to more directly cater to criminals in need of laundering cryptocurrency.[25] With strong compliance programs, these domains carry, at best, moderate to high levels of risk. Other domains, such as institutional exchanges and depository institutions, have more legitimate bases for their business models. As such, even though they can be involved in large amounts of money laundering activity, this is a result of either high volumes of trading or weak compliance programs. But the business model itself can be justified by the existence of many non-criminal reasons why customers use the offered services. The risk for these domains, therefore, depends more on the nature of their respective compliance program and not the business model itself.

With this in mind, we can categorize the risk profiles of the primary domains of cryptocurrency money laundering. Notably, even with robust compliance programs, certain high-risk domains, such as P2P exchangers and mixing services, still pose moderate or high-risk profiles.

---

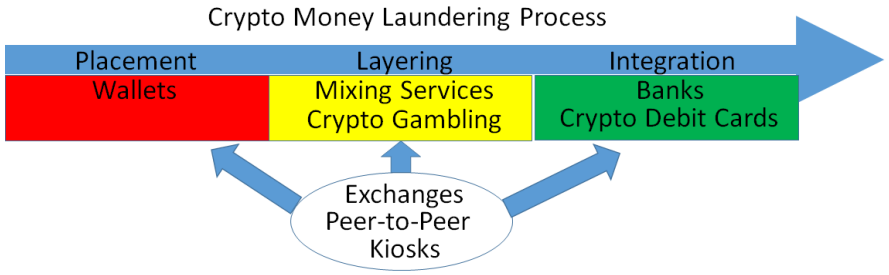
[24] Terence Zimwara, *Kucoin Hack: $17M Laundered Via Decentralized Exchanges, Blockchain Analysis Firm Claims this Can Still Be Traced*, BITCOIN.COM (Oct. 2, 2020), https://news.bitcoin.com/kucoin-hack-17m-laundered-via-decentralized-exchanges-blockchain-analysis-firm-claims-this-can-still-be-traced/.

[25] CHAINALYSIS, *supra* note 5, at 9 ("[R]isky services include [peer-to-peer] exchanges, mixing services, high risk exchanges, and gambling sites.").



From a long-term perspective, as cryptocurrency becomes more widely adopted, it will become less likely that run-of-the-mill cryptocurrency transactions will be associated with money laundering. In the early days of cryptocurrency, a great deal of activity was tied to illegal conduct on the dark web, which is why the shuttering of dark web marketplaces could impact the value of bitcoin. But as mainstream adoption of cryptocurrency has grown, the percentage of transactions used to promote or conceal crime has also decreased.[26] In this sense, cryptocurrency sectors not catering to money laundering, such as compliant institutional exchanges, will likely service less and less criminals as a percentage of their business. The same cannot be said for other sectors.

The various domains described below typically appear at different parts of the money laundering process. Let's discuss the examples described above, where criminals obtain their ill-gotten gains as



[26] *Id.* at 27.

cryptocurrency and convert it to fiat currency for use in the kinetic world. To first possess cryptocurrency, criminals must set up wallets. Those wallets might be under their exclusive control, or they might be custodial wallets hosted by a third-party service provider, such as an institutional exchange. Once in a wallet, funds can be sent to mixing services or gambling sites to obscure their historical trail. From there, the funds can be converted to fiat currency through exchanges, P2P exchangers, or kiosks. Sometimes, the funds will then be sent to bank accounts or cryptocurrency debit cards where they can be used to buy things or pay off debts. While this is the typical way in which the primary domains appear in the PLI process, criminals can use the domains in almost any way they want: Wallets can be used to mix funds; P2P exchangers can be used to integrate the funds; and kiosks can be used for layering. Criminals can also repeat the steps of the PLI process to further obfuscate the origin of the ill-gotten funds, though they incur additional costs and risk every time they repeat the cycle.

A note on professional money laundering and third-party money launderers

The Financial Action Task Force (FATF)[27] defines third-party money laundering as the laundering of proceeds by a person who was not involved in the commission of the predicate offence.[28] Further, the FATF denotes the most unique characteristic of professional money laundering (PML) is laundering for profit.[29] PMLs and other third-party money launderers are generally not directly involved in the predicate offense but serve to separate the criminals committing

---

[27] The FATF is an intergovernmental organization founded in 1989 on the initiative of the G7 by the ministers of its member jurisdictions. Its objectives are to set standards and to promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, proliferation of weapons of mass destruction, and other related threats to the integrity of the international financial system. *What We Do*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/about/whatwedo/ (last visited May 10, 2021).

[28] FIN. ACTION TASK FORCE, METHODOLOGY FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS 116 n.100 (Nov. 2020).

[29] FIN. ACTION TASK FORCE, FATF REPORT: PROFESSIONAL MONEY LAUNDERING 10 (July 2018).

the predicate offense from their illicit proceeds before returning unrelated funds, less a fee. Just like in traditional money laundering spheres, PMLs may exploit these platforms, software, and services. And just like in traditional money laundering spheres, there exist PMLs within each of the areas described below. Crypto-laundering is, after all, simply money laundering with a technological twist.

A. Wallets

Nothing can begin or end in the world of cryptocurrency without a wallet. A wallet is fundamentally the virtual equivalent of an account. Most wallets serve as an interface with blockchains and generate and store the public and private key pairs necessary to send and receive cryptocurrency.[30] Cryptocurrency wallets can be housed in a variety of forms, including on a tangible, external device ("hardware wallets"); downloaded as software onto either a personal computer, server, or smartphone ("software wallets"); printed public and private keys ("paper wallets"); and as an online account associated with a cryptocurrency service provider such as an exchange.[31]

1. Who holds the keys?

If the end user has sole access to the private keys, the wallet is considered non-custodial or *unhosted.* Hardware and paper wallets are always unhosted; they are often referred to as *cold storage* wallets.[32] Alternatively, if a third-party wallet provider, such as an exchange, holds the private keys, the wallet is considered custodial or a *hosted* wallet provider. Software wallets may be hosted or unhosted. Many unhosted wallet providers will not be considered money transmitters or virtual asset service providers (VASPs) subject to record keeping and reporting requirements like other financial institutions.[33] Unhosted wallets create a situation similar to an

---

[30] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 3.

[31] *Id.*

[32] "Cold storage" refers to a wallet that is not connected to the Internet. Hardware devices that provide cold storage wallets can, however, be connected to the internet in order to make transfers in and out.

[33] Virtual Asset Service Provider, or VASP, is the term used by the FATF to describe the FATF Standards' covered entities performing certain financial activities involving virtual assets such as cryptocurrency. A VASP is the functional equivalent of the U.S. BSA's MSB or money transmitting business. VASPs, however, may be defined broader in some jurisdictions. *See* FIN.

individual carrying cash in a billfold or storing it under a mattress. To connect an individual to a billfold full of cash or an unhosted wallet, law enforcement must associate the individual to the assets in some way, such as physical possession or control of the wallet or through transaction tracing back to a point of attribution. The way unhosted wallet software is designed can vary and affect what type of transactional information may be available. In the case of such non-custodial or unhosted wallets, investigators may be dependent on the owner's willingness to cooperate, or the discovery of keys, seeds, and login passwords during device and house searches to access these wallets.

2. Mixing-enabled wallets

The custodial nature of many dedicated mixing services raises significant trust issues for individuals.[34] Is the service going to run off with the money? Will it run into technical difficulties and prevent the funds from being returned? Will the service providers comply with law enforcement or—worse—will law enforcement seize the service?

For the criminal who cannot move past these questions, other mixing options exist in the form of mixing-enabled wallets (MEWs). MEWs may be hosted or unhosted. MEWs integrate a mixing protocol into the wallet so that the end user can automatically, or have the option to, *mix* their funds before withdrawal.[35] Unhosted MEWs may involve a fee paid to an administrative entity for coordinating the mixing across its user base.[36]

These protocols and proofs, when integrated with a service or software, enable the laundering of funds in an automated fashion and do not offer another financially beneficial function. This makes these services particularly attractive for criminals wishing to conceal or

---

ACTION TASK FORCE, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 130 (2020).

[34] Tom Robinson, *Over 13% of All Proceeds of Crime in Bitcoin are Now Laundered Through Privacy Wallets*, ELLIPTIC BLOG (Dec. 9, 2020), https://www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet.

[35] Kai Sedgwick, *How to Mix Your Bitcoins Using CoinJoin for Greater Privacy*, BITCOIN (Mar. 3, 2020), https://news.bitcoin.com/how-to-mix-your-bitcoins-using-coinjoin/.

[36] *Id.*; *PrivateSend and InstantSend*, DASH, https://docs.dash.org/en/stable/wallets/dashcore/privatesend-instantsend.html (last visited May 10, 2021).

disguise the nature, location, source, ownership, or control of illicit proceeds. The use of mixing services or MEWs could arguably provide evidence of concealment.

B. Institutional exchanges

One of the first exchanges was the infamous Mt. Gox, a fantasy card trading platform that morphed into the world's largest cryptocurrency exchange at the time. Led by French programmer Mark Karpeles, Mt. Gox dominated the early cryptocurrency market, handling an estimated 70% of all transactions on the Bitcoin blockchain.[37] Things didn't go well for Karpeles. The company closed in early 2014 after an estimated 744,000 bitcoins—about 6% of the total 12.4 million bitcoins in circulation at the time—were stolen from the company's wallets.[38] Karpeles was eventually prosecuted by Japanese authorities for falsifying data related to the exchange's accounts.[39]

From this inauspicious beginning, cryptocurrency exchanges became a mainstream platform through which cryptocurrency can be bought, sold, and custodied. Cryptocurrency exchanges operate like online banks. Customers open accounts with a variety of identification documents, and once verified, they can exchange fiat money for cryptocurrency, and vice-versa. While exchanges look and feel like online banks, they typically service a much broader set of customers. Most banks have some connection to their customers' physical location, even if it is an international bank. Customers typically have to open accounts in-person at a bank branch, and a routing number associated with that branch is assigned to the customers' accounts. This is not so with exchanges, which may service customers throughout the world without any physical connection to the location of the exchange. Indeed, exchanges do not have brick and mortar branches where know-your-customer checks can be conducted. Rather, a customer will typically onboard by providing identifying information over the internet. This is not to say that institutional exchanges don't conduct KYC checks after an account is opened, but rather that this is

---

[37] MARIUS-CRISTIAN FRUNZA, SOLVING MODERN CRIME IN FINANCIAL MARKETS: 65 (2015).

[38] *Id.* at 65.

[39] Kasaku Narioka & Takashi Mochizuki, *Former Mt. Gox Bitcoin Bigwig Unlikely to Do More Jail Time After Beating Embezzlement Charges*, WALL ST. J. (Mar. 15, 2019), https://www.wsj.com/articles/former-mt-gox-bitcoin-bigwig-found-guilty-wont-likely-do-time-11552613358.

never accomplished via an in-person meeting. Even so, institutional exchanges appear to carry less inherent money laundering risk because the business model isn't premised on charging a money laundering premium. Considering the low fees exchanges charge, it makes sense that individuals interested in legally purchasing or transacting in cryptocurrency would turn to an institutional exchange to deal in these virtual assets. The problem with institutional exchanges is when they fail to maintain adequate anti-money laundering controls. Sometimes, this happens because exchanges directly cater to the criminal element, as was the case with BTC-e,[40] but sometimes, it's simply the result of exchanges being inexperienced or unwilling to spend resources on an adequate compliance program. These failures aren't unique to institutional exchanges, as traditional banks have also been prosecuted for engaging in shoddy anti-money laundering practices for decades.

The larger issue associated with institutional exchanges is when they engage in jurisdictional arbitrage. As noted above, because exchanges don't maintain physical bank branches to operate, it's easy for them to "move around." An exchange can base its operations in an offshore jurisdiction with weak anti-money laundering regulations but still service customers throughout the world. While this doesn't make them immune from U.S. regulations if they service U.S. customers, it can make it more difficult for law enforcement to issue service of process on them and to investigate them. In sum, institutional exchanges don't pose an inherent money laundering risk, but the devil is in the details of how they operate. The broad reach of an institutional exchange means that any failures in its anti-money laundering program can be quickly exploited by criminals throughout the world. For this reason, it is crucial that institutional exchanges maintain robust anti-money laundering programs to compensate for the unusually broad reach of customers they service.

---

[40] Press Release, U.S. Att'y's Off. N. Dist. Cal, Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack of Mt. Gox (July 26, 2017).

C. Over-the-counter brokers

Over-the-counter (OTC) brokers are a type of MSB that facilitate significant trades between buyers and sellers.[41] While OTC traders maintain accounts at one or several exchanges for liquidity purposes, their customers need not register with the exchange.[42] These are also called *nested services* in that they tend to operate within one or more larger exchanges.[43] Depending on the OTC broker, a customer may only be required to provide minimal or no KYC information.[44] Criminals may seek out OTC traders because they cannot obtain accounts at exchanges or are unwilling to risk having their funds frozen.[45] In its 2020 Crypto Crime Report, Chainalysis identified the "Rogue 100," a group of OTC brokers it believes to be involved in money laundering activity. Chainalysis stated that just the funds received by these 100 OTC brokers "can account for as much as 1% of all Bitcoin activity in a given month." Chainalysis further noted that, "the money laundering infrastructure driven by OTC brokers enables nearly every other type of crime" covered in the report.[46] Kaiko, a cryptocurrency market data provider, estimated that OTC brokers could facilitate the majority of all cryptocurrency trade volume.[47]

OTC broker case study: North Korean thefts

In August 2020, the United States forfeited cryptocurrency accounts related to three North Korean hacking incidents. According to the complaint, the hacker stole over $250 million worth of alternative cryptocurrencies and tokens, including Proton Tokens, PlayGame tokens, and IHT Real Estate Protocol tokens. The hacker then used multiple virtual asset laundering methods to obfuscate his trail, but ultimately, laundered his illicit proceeds through Chinese OTC actors,

---

[41] Complaint at 12, United States v. 280 Virtual Currency Accounts, No. 20-cv-2396 (D.D.C. Aug. 27, 2020), ECF No. 1.

[42] CHAINALYSIS, *supra* note 5, at 12.

[43] THE 2021 CRYPTO CRIME REPORT, *supra* note 17, at 13.

[44] Complaint, *supra* note 40, at 12.

[45] *Id.*

[46] CHAINALYSIS, supra note 5, at 13–15.

[47] Clara Medalie, *What is OTC Cryptocurrency Trading?,* KAIKO (Apr. 2, 2019), https://blog.kaiko.com/what-is-otc-cryptocurrency-trading-66d725c867f.

who failed to keep KYC records. Despite these attempts to launder the funds, law enforcement traced the funds to the forfeited accounts.[48]

D. P2P exchangers and platforms

A man walks into a Starbucks. He is a peer-to-peer cryptocurrency exchanger. He orders a latte, sits down at a table, and waits for his customer to arrive. The customer walks in and sits down; he has a duffle bag containing $100,000 in cash. The exchanger covertly inspects the cash and then sends $100,000 in bitcoin to a wallet address provided by the customer. They wait for the transaction to be confirmed on the blockchain and then part ways. The customer pays a higher exchange rate as the cost of doing business with an exchanger who will not file a SAR on the transaction. No questions asked; no information reported. This may seem far-fetched, but this type of activity happens daily in cities and towns all over the world, in much larger amounts, and these exchangers often operate on either side of the transaction—both buying and selling millions of dollars' worth of cryptocurrency. It is an effective money laundering scheme unless the P2P exchanger or his customers seeking to stay anonymous get caught.[49]

The business model of P2P exchanging is premised on money laundering. This doesn't mean that all P2P exchangers are money launderers, but rather that the success of the business model depends on it. Otherwise, why would anyone go through the hassle of meeting someone in person to buy or sell cryptocurrency when they could do it online through a registered exchange? On top of the hassle, most exchanges charge less than 2% per transaction, while P2P exchangers often charge between two and six times that rate. Even worse than the hassle and cost, individuals risk being robbed while engaging in face-to-face exchanges. Customers endure this risk, cost, and hassle because they want no questions asked when they buy or sell cryptocurrency—they do not want to provide identification to an exchange, and they do not want a financial institution filing a SAR or a CTR. In other words, they are willing to pay a money laundering

---

[48] Press Release, U.S. Dep't of Justice, United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors (Aug. 27, 2020).

[49] *See* Press Release, U.S. Att'y's Off. Cent. Dist. Cal., "Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case (July 9, 2018).

premium. Both FinCEN's Advisory and the FATF guidance on money laundering red flags in cryptocurrency transactions include this exact scenario as a red flag, namely, when a P2P exchanger "handle[s] huge amount[s] of [cryptocurrency] transfers on its customer's behalf, and charge[s] higher fees to its customer than transmission services offered by other exchanges."[50] This premium keeps the business model going, as P2P exchangers continue to operate illegally even with the risk of civil or criminal fines under the money laundering statutes and the Bank Secrecy Act.[51]

In addition to criminals, victims of ransomware attacks have relied on P2P exchangers. With the rise of ransomware as a standardized criminal enterprise, an increasing number of victims have been forced to purchase cryptocurrency in short order.[52] It has been estimated that 9% of Bitcoin transactions are attributable to ransomware or some other form of cyber extortion payment.[53] If it takes days or weeks to open a validated account at an institutional exchange, a P2P exchanger can offer cryptocurrency at a moment's notice, and victims are willing to pay this speed premium. Victims have noted that "the processing times [at a registered institutional exchange] were far beyond the scope of the immediacy posed by the ransom" and that a P2P exchanger was a better option for obtaining cryptocurrency in a hurry.[54]

---

[50] FIN. ACTION TASK FORCE, VIRTUAL ASSETS RED FLAG INDICATORS OF MONEY LAUNDERING AND TERRORIST FINANCING, 9 (Sept. 2020).

[51] *See* Assessment of Civil Money Penalty, *In re* Eric Powers, 2019-01 (U.S. Dep't of the Treasury Apr. 18, 2019).

[52] The current business model involves criminal developers selling to customers through a partnership program. This is referred to as RaaS (Ransomware as a Service) and is a primary reason for the explosion of ransomware attacks. Attackers no longer have to develop their own ransomware, but instead can rely on specialists to develop the programs that the attackers then use. CROWDSTRIKE, 2020 GLOBAL THREAT REPORT 15, 19–20 (2020).

[53] Maria Korolov, *Don't Pay Ransoms. But if You Must, Here's Where to Buy the Bitcoins*, CSO (Apr. 4, 2017), https://www.csoonline.com/article/ 3186493/ dont-pay-ransoms-but-if-you-must-heres-where-to-buy-the-bitcoins.html.

[54] Bryce Bearchell, Ransomware: the anatomy of paying a ransom to decrypt hostage files, Coalfire (May 2017), https://www.coalfire.com/the-coalfire-blog/ may-2017/ransomware-the-anatomy-of-paying-a-ransom.

Law enforcement has successfully prosecuted P2P exchangers for money laundering and violations of the BSA, but these cases are exceptions to the norm of P2P exchangers operating with impunity. Law enforcement has limited resources and simply cannot investigate every P2P exchanger operating outside of the law. Another method for dealing with P2P money laundering is focusing on the platforms used by P2P exchangers. These platforms often operate like Craigslist, allowing P2P exchangers to advertise cryptocurrency they want to buy or sell. Most of these services operate an escrow service for transactions conducted through the site to minimize scamming. Without these sites, P2P exchangers would struggle to advertise their services and conduct trades in an efficient manner. In return for providing these services, P2P exchange sites often charge a fixed or percentage-based fee for every transaction conducted through their platforms.

By not just passively providing a communication forum, these sites may be considered money transmitters subject to the Bank Secrecy Act and related regulations.[55] Moreover, sites offering custodial, or hosted, wallets are more likely money services businesses (MSBs) under the law in the United States and VASPs according to the FATF Recommendations.[56] Customers of these platforms pay a premium for anonymity, and KYC policies defeat the anonymity that many customers seek, which is why these platforms rarely maintain robust compliance programs. Stronger enforcement measures against these

---

[55] Guidance, Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019) [hereinafter 2019 Guidance].

[56] David E. Teitelbaum & Lilya Tessler, Financial Action Task Force Guidance Regarding Digital Asset Exchanges, ICOs, DApps, Wallets and More, SIDLEY (July 1, 2019), https://www.sidley.com/en/insights/newsupdates/2019/07/financial-action-task-force-guidance-regarding-digital-asset-exchanges ("A VASP is defined as any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies, (ii) exchange between one or more forms of virtual assets, (iii) transfer of virtual assets, (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.").

types of platforms would likely curb the flow of P2P-facilitated money laundering.

P2P exchanger case study: Operation Dark Gold

In 2018, the Department of Justice (Department) and multiple federal law enforcement agencies announced the results of a year-long, coordinated national operation dubbed Operation Dark Gold.[57] Investigators used the popular P2P exchanger business model to target vendors of illicit goods on the Darknet. Posing as a cryptocurrency money launderer on Darknet market websites, undercover investigators exchanged U.S. currency for cryptocurrency with numerous vendors of illicit goods, leading to the identification and prosecution of scores of these individuals across the country. The undercover exchanger received cash from these criminals through the mail, and investigators were able trace the cryptocurrency received from them back to their illicit activities. In addition to the take down of these targeted vendors, the Department seized over $25 million in cash, gold, and cryptocurrency, as well as drugs, guns, and a grenade launcher.[58]

E. Mixing services

In the 1990s, groups of tax dodgers began using a scheme called warehouse banking, in which a dirty bank would commingle all deposits into a single account to conceal the ownership of the funds. When a depositor withdrew funds from the account, it was impossible to trace where those funds came from. Eventually, these schemes were shut down, and the organizers were prosecuted for tax and money laundering violations.[59] Mixing services are the warehouse banking of cryptocurrency: Funds are sent to the mixing service, where they are commingled with other funds and then sent to a designated wallet

---

[57] Press Release, U.S. Dep't of Justice, First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than $23.6 Million (June 26, 2018); Aaron Katersky & Luke Barr, *Authorities Arrest 40, Seize More Than $3.6 Million in Gold Bars in 1st Darknet Bust*, ABC NEWS (June 27, 2018), https://abcnews.go.com/Politics/authorities-arrest-40-seize-36-million-gold-bars/story?id=56200805.

[58] Press Release, *supra* note 56.

[59] Press Release, U.S. Dep't of Justice, Federal Court in Seattle Shuts Down So-Called "Warehouse Bank" (May 1, 2007).

address in the same or different form of cryptocurrency.[60] While these services claim to have legitimate purposes, such as enhancing a user's privacy while engaging in cryptocurrency transactions, money laundering is a main component of their operations.

The below graphic explains how a criminal might launder funds through a dedicated mixing service.

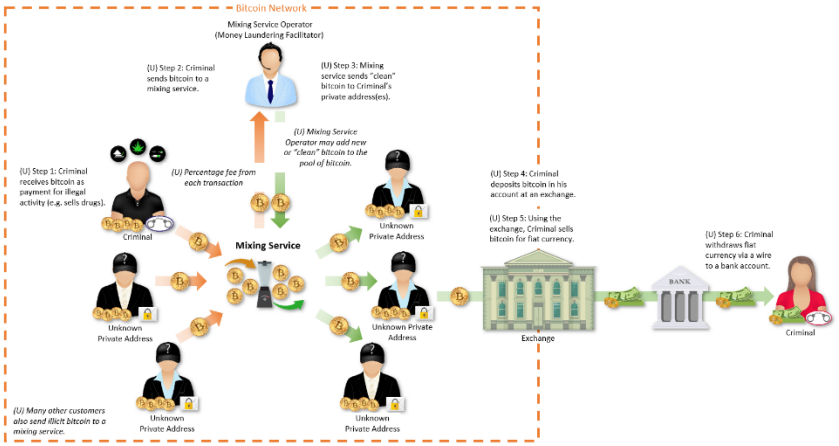


Figure 1: Example of a Criminal "Mixing" Enterprise[61]

Even with a business model based on money laundering, mixing services may be obligated to maintain anti-money laundering programs and respond to records requests from law enforcement.[62] As such, they aren't always a black box for law enforcement and may in fact provide useful information for criminal investigations. All of the risks associated with institutional exchanges also exist with mixing services: They can jurisdiction hop; they can service clients globally; and they likely lack the necessary anti-money laundering (AML) compliance systems and staff to keep up with inherent risks in their business model. Nevertheless, it is theoretically possible that a mixing service could comply with U.S. regulations if it maintained a sufficient anti-money laundering program.

Mixing services case study: Bitcoin Fog

In April 2021, federal prosecutors charged a dual Russian–Swedish national for his alleged operation of the longest-running bitcoin money

---

[60] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 41.
[61] *Id.* at 42.
[62] 2019 Guidance, *supra* note 54.

laundering service on the Darknet.[63] According to court documents, the defendant operated Bitcoin Fog, a cryptocurrency "mixer," gaining notoriety as a go-to money laundering service for criminals seeking to hide their illicit proceeds from law enforcement.[64] The criminal complaint filed in the District of Columbia alleged that since 2011, Bitcoin Fog moved over 1.2 million bitcoin—valued at approximately $335 million at the time of the transactions, and the bulk of this cryptocurrency came from Darknet marketplaces and was tied to illegal products and services.[65]

F. Cryptocurrency kiosks

It is estimated that, as of April 2021, there are over 19,000 cryptocurrency kiosks globally.[66] Like other high-risk cryptocurrency platforms, cryptocurrency kiosks may provide an effective vehicle for money laundering. Kiosks operate like ATM machines. Customers go to physical machines, often located in easily accessible locations like shopping malls or gas stations, and use the machines to purchase or sell cryptocurrency. Customers often pay exorbitant premiums to use kiosks, much like the premiums charged by P2P exchangers. Because cryptocurrency kiosks have only recently become popular, enforcement actions have been rare. Until the cryptocurrency kiosk industry has been educated, and perhaps tamed, by regulators and law enforcement, it will remain a popular tool for a wide variety of criminal activity. Kiosks have been heavily used by individuals and entities that promote, facilitate, and profit from sex trafficking because cryptocurrency has increasingly been used to pay for websites that advertise commercial sex.[67] One of the reasons for the increased use of cryptocurrency is that major merchant processors, like Visa and Mastercard, no longer allow transactions to pay for or host

---

[63] Press Release, U.S. Dep't of Justice, Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer" (Apr. 28, 2021).

[64] *Id.*; Criminal Complaint, United States v. Sterlingov, 21-mj-400, (D.D.C. Apr. 26, 2021), ECF No. 1.

[65] Criminal Complaint, supra note 63.

[66] *Bitcoin ATM Installations Growth*, COIN ATM RADAR (Apr. 30, 2021), https://coinatmradar.com/charts/growth/.

[67] REBECCA S. PORTNOFF, *ET AL.*, BACKPAGE AND BITCOIN: UNCOVERING HUMAN TRAFFICKERS 2 (Aug. 2017) ("[S]urveys all found that the majority of US-based trafficking victims are advertised online.").

advertisements websites, such as the government-seized Backpage.[68] In some cases, traffickers or victims of trafficking under the direction of their trafficker will change the form of the illicit proceeds from cash to cryptocurrency at kiosks and then use the cryptocurrency to further promote the illegal activity.

Another reason why traffickers prefer using cryptocurrency kiosks is their ability to avoid the KYC requirements of regulated institutional exchanges. While kiosk companies fall squarely within the same set of BSA regulations, they often operate without sufficient AML controls.[69] This allows their customers to carry out transactions, particularly small ones that are used to pay for advertisements for commercial sex, without providing any identification. Often, victims of sex trafficking may not have access to bank accounts, or in some instances, traffickers open bank accounts using the victims' names. By using kiosks, the traffickers can also avoid linking any bank accounts or a financial footprint as would be required if they used traditional financial institutions or institutional exchanges.

Kiosks are also commonly used by dark web market vendors of illicit products, including drugs, firearms, and stolen identity information, who are looking to offload the payments they received from customers in cryptocurrency.[70] They can tolerate the high premiums as a reasonable price to pay for anonymity. Moreover, operating one or more kiosks may offer such vendors a lucrative method for converting illicit proceeds from cryptocurrency back into fiat currency. This isn't to say that vendors only use kiosks. Rather, vendors often use the full scope of domains described in this article. If one of their accounts is closed, they can easily move to another domain.

Finally, kiosks may facilitate cryptocurrency payments in fraud and extortion schemes in which victims are directed to use kiosks to easily and quickly obtain and send cryptocurrency to perpetrators. In sum,

---

[68] *Id.* at 3 ("On July 1, 2015, Visa and Mastercard stopped processing transactions for adult listings on Backpage, which caused Backpage to switch to Bitcoin payments for all paid adult ads.").

[69] 2019 Guidance, *supra* note 54.

[70] *See, e.g.,* Press Release, U.S. Att'y's Off. Cent. Dist. Cal., Westwood Man Agrees to Plead Guilty to Federal Narcotics, Money Laundering Charges for Running Unlicensed Bitcoin Exchange and ATM (Aug. 23, 2019); Press Release, U.S. Att's' Off. Cent. Dist. Cal., O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit (July 22, 2020).

cryptocurrency kiosks are high-risk enterprises, even with robust compliance programs.

G. Traditional financial institutions

Traditional financial institutions often play a significant role in cryptocurrency money laundering because, in the end, criminals want to convert their ill-gotten cryptocurrency into fiat currency—and the most useful and common place to maintain fiat currency is in a depository institution.[71] When ill-gotten funds are converted to fiat currency and sent to a bank for safekeeping, criminals can continue to *layer* (by sending the funds to other locations) or they can begin the *integration* process (by purchasing goods or paying off debts).

Banks will often see funds sent to or from institutional exchanges because the exchanges often require customers to provide a bank account as part of the onboarding process. The exchange customer uses the linked bank account to pay for cryptocurrency purchases and to receive the proceeds of cryptocurrency sales. This activity should be easy for a bank to identify, as it can determine if the recipient is an institutional exchange. Based on this information, the bank can make individualized risk assessments about its customers. As such, a bank with a sufficient compliance program should be able to incur tolerable risk when servicing customers engaged in cryptocurrency transactions.

A bank's risk levels may increase, however, if its customers are P2P exchangers, who often use banks to send or receive payments (or to deposit or withdraw cash). A robust AML program should pick up on a customer engaged in this type of activity because it will trigger red flags, including unexplained cash deposits and withdrawals and wire transfers with unknown business purposes. This type of suspicious conduct should cause a bank to inquire with the customer as to the source of funds. If the customer can't explain her business practices, the accounts likely should be closed by the bank.

What are the common financial patterns of P2P exchangers? It depends on if they are selling or buying cryptocurrency, though, often,

---

[71] Joshua Mapperson, *FinCEN Director Warns Banks About Cryptocurrency Risk Exposure*, COINTELEGRAPH (Sept. 30, 2020), https://cointelegraph.com/news/fincen-director-warns-banks-about-cryptocurrency-risk-exposure ("[B]anks must be thinking about their crypto exposure as well.") (quoting FinCEN Director Ken Blanco).

they will do both as a means of triaging bear and bull cryptocurrency markets. If the P2P exchanger is purchasing cryptocurrency from customers, bank records will show a wire transfer or other payment method to a series of random individuals (the P2P exchanger's customers). Without additional information about the customer, it might be difficult for the bank to determine the purpose of such debits. In addition to direct payments, P2P exchangers will also operate in cash. This means that their bank accounts will often show regular, large cash deposits or withdrawals. After the P2P exchanger purchases the cryptocurrency, she may send it to an institutional exchange, where it will be sold. The profits are then transferred back to the P2P exchanger's bank account. It is not uncommon, therefore, for P2P exchangers to regularly receive large domestic and international wire transfers from institutional exchanges.

If the P2P exchanger is selling cryptocurrency, she will likely receive regular payments from customers or make regular cash deposits into her accounts. Sometimes that deposited cash is used to buy more cryptocurrency from an institutional exchange, and the cycle begins again. But as noted above, P2P exchangers will often both buy and sell cryptocurrency, so their bank account records will likely show a combination of these transaction patterns.

Should a bank automatically close an account when it learns that a customer is a P2P exchanger? No single answer is correct. It is, in theory, possible for a P2P exchanger to operate within the law. She would have to be a licensed money transmitter, both federally and at the state level; would have to maintain an anti-money laundering compliance program; and would have to file SARs and CTRs. If all these requirements are met, a bank might be able to justify the potential risks of servicing a customer engaged in this business activity.

H. Cryptocurrency debit cards and payment apps

Just as criminals have used credit cards, debit cards, and gift cards to facilitate unlawful activity, conceal illicit financial flows, and use these methods of payment to integrate ill-gotten gains, debit cards and payment apps funded by or supporting cryptocurrency transactions may also be used to launder money.

Cryptocurrency payment processors operate in a familiar manner to other fiat-sourced payment apps. These companies provide software allowing retail merchants to accept cryptocurrencies as payment online or in brick-and-mortar establishments. Generally, the

merchants do not handle cryptocurrencies directly. Rather, customers fund their payment app wallet or debit card with cryptocurrency, and the processor converts the cryptocurrency into fiat currency. The processor then sends those converted funds to the merchant, minus a commission.[72] Like exchanges and kiosks, most payment processors are MSBs with BSA record keeping and reporting requirements.[73] Thus, their KYC and transactional records can be an important source for leads and evidence in financial investigations.

Examples of established fiat payment processors now offering varying services in cryptocurrency are PayPal (including Venmo) and Square (d/b/a CashApp). Many national retailers like Home Depot and Whole Foods accept Flexa, a payments network supported by various cryptocurrency payment apps.[74] In addition, many companies, including exchanges and payment processors, offer visa debit cards funded with cryptocurrency account balances.[75] Like fiat-funded debit cards, these cards can be used to pay for anything online or in person or used to make ATM cash withdrawals. For a more detailed discussion of these new technologies, the authors recommend *Money Moves: Following the Money Beyond the Banking System*.[76]

I. Cryptocurrency gambling websites

These online gambling platforms or "casinos" that facilitate various forms of betting denominated in bitcoin and other cryptocurrencies are increasingly used for money laundering. Under current law, a casino that has gross annual gaming revenue in excess of $1 million, regardless of denomination in cryptocurrency or other value, must be duly licensed and authorized to do business as a casino in the United States by a federal, State, or tribal authority. Casinos that do not meet this criterion may be considered MSBs and subject to the

---

[72] Yaya J. Fanusie, *Merchant Crypto Payments: A New National Security Frontier*, LAWFARE (Mar. 24, 2021), https://www.lawfareblog.com/merchant-crypto-payments-new-national-security-frontier.

[73] 2019 Guidance, *supra* note 54.

[74] *The Global Leader in Pure-Digital Payments*, FLEXA, https://flexa.network/ (last visited May 10, 2021).

[75] Robert Stevens, *The Best Bitcoin Debit Cards to Use in 2021*, DECRYPT (Dec. 2, 2020), https://decrypt.co/47104/best-bitcoin-debit-cards.

[76] Elizabeth Boison & Leo Tsao, *Money Moves: Following the Money Beyond the Banking System*, 67 DOJ J. FED. L. & PRAC., no. 3, 2019, at 93.

BSA and its KYC record keeping and reporting requirements, nonetheless.[77]

Criminals may launder their illicit proceeds through cryptocurrency gambling sites as a layering technique. On these sites, users may send their dirty cryptocurrency to the online casino, trading them for virtual chips or credit.[78] Whether the criminal chooses to gamble any of their funds is up to them, but otherwise the virtual chips or credit may then be cashed out into a virtual asset and withdrawn.

V. Following the crypto: potential on-chain layering techniques

A. A note on blockchain analysis

It is possible, using the Bitcoin blockchain, to trace funds forwards and backwards from a single address or a single transaction, not unlike the manner in which investigators trace the movement of funds in fiat currencies. Unlike a traditional bank statement, however, the record on a blockchain for a particular bitcoin address often contains only a single incoming and single outgoing transaction, due to the practice of depositing leftover funds in a new *change address*. In these instances, it becomes necessary to identify the sequence of subsequent and prior payments to trace the disposition of funds associated with a single actor. Additionally, unlike more traditional bank records, the blockchain does not identify the sender or receiver, apart from the public addresses. Investigators can sometimes obtain this information from serving legal process to MSBs and VASPs. In this way, it is often possible for investigators to identify payment streams—that is, a single flow of funds over time—believed to involve the same pool of funds controlled by a particular person or persons. As a result, blockchain analysis is a crucial technique for investigating virtual assets.

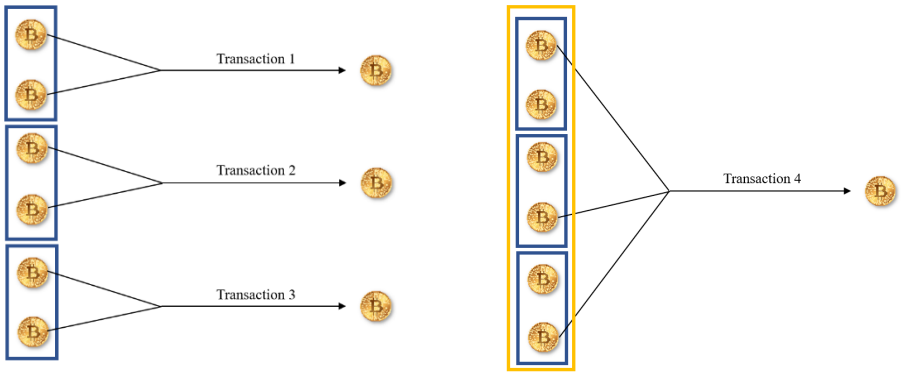
One of the most common techniques involved in blockchain analysis is co-spend analysis, sometimes referred to as "common input analysis." Co-spending occurs when multiple inputs are used to send

---

[77] 31 C.F.R. § 1010.100(t)(5)(i), (6); *see also* CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 39–41; 2019 Guidance, *supra* note 54, at 23. [78] *Bitcoin Money Laundering: How Criminals Use Crypto*, ELLIPTIC (Sept. 18, 2019), https://www.elliptic.co/blog/bitcoin-money-laundering.

bitcoin in a single transaction, indicating that a single owner holds the private keys for all those addresses.

For example, six disparate Bitcoin addresses found in an investigation may, on their face, appear unrelated. A quick search of an open source blockchain explorer reveals transactions associated with these addresses. But what can those transactions tell us? By analyzing the transactions using co-spend analysis, the investigator may connect the dots to determine that all the addresses belong to the same wallet. The following graphic shows how three transactions can associate six disparate addresses into three separate wallets.



Figures 2 and 3: Illustrations of Co-spending Transactions

But what if the investigator were to find an additional transaction involving three inputs from an address in each of the above wallets?

The investigator may then demonstrate that each of the original six disparate addresses are a part of the same wallet. This analytic technique, when combined with traditional investigative steps, may provide valuable insight. Armed with blockchain analysis and traditional investigative tools, investigators may leverage this information to determine the breadth of the scheme, the value of the assets, cash out points, and even the identity of criminal actors.

B. Anonymity and privacy-enhanced cryptocurrencies

Sometimes, the money laundering vehicle is the cryptocurrency itself. As detailed above, while Bitcoin provides for a public and transparent blockchain, a number of cryptocurrencies are designed with blockchains that enhance the privacy of transactions; these cryptocurrencies are often referred to as anonymity-enhanced cryptocurrencies (AECs) or *privacy coins*. The Department considers

the use of AECs to be indicative of possible criminal conduct and generally does not liquidate seized or forfeited AECs.[79]

Although cryptocurrency addresses do not have names or specific customer information attached to them, because many blockchains are public, users can query addresses to view and understand the transactions to some extent. AECs, however, use non-public or private blockchains, or built-in mixing protocols, that make it more difficult to trace or attribute transactions. Like sharks to chum, criminals seek out privacy to conceal their conduct, and AECs offer these additional features for concealing value transfer. In terms of the PLI process, AECs make layering inherent to all transactions and, therefore, are an efficient method for this part of the money laundering process.

AECs and privacy coins may use various non-interactive zero-knowledge proofs as a part of the underlying technology to facilitate the transfer of value. For example, ZCash private and shielded transactions use zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) proofs to encrypt the involved private address(es).[80] Private transactions will also encrypt the transaction amount and memo field.[81] Monero uses *Bulletproofs*, another type of non-interactive zero-knowledge proof.[82] *Non-interactive zero knowledge proofs* are a type of zero-knowledge proof in which the *prover* sends one message to the *verifier* in which the prover demonstrates to the verifier that they know something. This is done without the prover conveying any information apart from the fact that

---

[79] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 41.

[80] According to the ZCash website,

> Owners of shielded addresses can disclose transaction details for regulatory compliance or auditing. The owner has the option to disclose all incoming transactions and the memo field, but does not have access to the sender address unless identifying information is included in the memo field. Zcash will soon support full viewing keys that reveal all transaction values in and out of the address.

See How it Works, ZCASH, https://z.cash/technology/ (last visited May 10, 2021).

[81] *What are zk-SNARKs?,* ZCASH, https://z.cash/technology/zksnarks/ (last visited May 10, 2021); *How it Works*, *supra* note 79.

[82] *Bulletproofs*, MONERO, https://web.getmonero.org/resources/moneropedia/bulletproofs.html (last visited May 10, 2021).

they know that something.[83] When applied to the cryptocurrency space, this means that specific information about a transaction need not be given away, apart from a representation of ownership of funds.

C. Mixing

In a nutshell, successful mixing breaks any links between the originator and the destination.[84] There are several different protocols that may change the way the mixing is accomplished. One of the more commonly exploited by criminal actors is *CoinJoin.*[85]

CoinJoin is a trustless method for combining multiple payments from multiple spenders into a single transaction with multiple outputs, making it more difficult for outside parties to determine which spender paid which recipient or recipients.[86]

D. Chain hopping

The concept of layering is not new to criminals. This can take many forms in the traditional financial world, including wire transfers between bank accounts, often held in multiple names, at multiple banks, and in multiple countries or real estate investments. Within the virtual asset landscape, one of the more prominent forms of

---

[83] While this proof involves complex mathematics, the authors have attempted to simplify the topic for the reader. For information on the underlying mathematics, see *Non-Interactive Zero-Knowledge Proof Systems*. Alfredo De Santis et al., Non-Interactive Zero-Knowledge Proof Systems, *in* Advances in Cryptology, 52 (Carl Pomerance ed. 1988); *What Are zk-SNARKs*, ZCASH, https://z.cash/technology/zksnarks/ (last visited May 10, 2021); *How it Works*, *supra* note 79.

[84] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 153 (2016).

[85] Robinson, *supra* note 33.

[86] NARAYANAN, *supra* note 87, at 156; *see also Frequently Asked Questions*, DASH, https://www.dash.org/faq/ (last visited May 10, 2021) ("Dash offers optional transaction anonymity through a feature called PrivateSend. An improvement of CoinJoin, PrivateSend allows you to break up your Dash into specific denominations and "mix" these with other participants, thereby obscuring the origin of funds used in the final transaction. PrivateSend offers superior privacy to centralized mixing services because each round of mixing is facilitated by a different masternode, making it effectively impossible to track funds on the blockchain.").

layering is known as *chain hopping* or *swapping*.[87] This involves switching from one cryptocurrency or virtual asset, such as a token, to another to *break the chain*. By trading one type of virtual asset for another, the criminal *switches* blockchains, attempting to obfuscate the transaction origin and destination.[88] This is generally done via dedicated centralized services or in an automated fashion (for example, decentralized exchanges).

VI. State of the law on money laundering and cryptocurrency

U.S. law addresses money laundering through two main statutes: The Bank Secrecy Act and the Money Laundering Control Act. The former focuses on regulating financial gatekeepers, such as banks and MSBs, while the latter criminalizes money laundering itself. These two pillars of anti-money laundering law have proven their effectiveness in the face of the first wave of cryptocurrency-enabled money laundering. This section provides an overview of the BSA and the Money Laundering Control Act as they relate to cryptocurrency.

A. The Bank Secrecy Act

The BSA would be better titled the Bank *Anti*-Secrecy Act, as the goal of the law is to bring to light the flow of illicit money in the United States.[89] Passed in 1970, the BSA began as a modest attempt to assist law enforcement in tracking funds used by organized crime. Over the last fifty years, the BSA morphed into a fundamental pillar of the global anti-money laundering framework. FinCEN is the core regulator of the BSA, but only the Department has authority to enforce the criminal components of the BSA.

The BSA is based on the simple idea that certain gatekeepers, referred to as *financial institutions*, are required to file certain types of financial reports on their customers' transactions: SARs and CTRs. Non-financial institutions, such as merchants, are required to file a form 8300s, which is similar to a CTR but with different reporting thresholds. In addition, individuals and institutions are obligated to

---

[87] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 28, 42, 44; *see also* Complaint, *supra* note 40.

[88] Complaint, *supra* note 40.

[89] The BSA, codified at 31 U.S.C §§ 5313–26, is often referred to as "Title 31." Accompanying regulations to Title 31 are found at 31 C.F.R. Chapter X.

file currency and monetary instrument reports (CMIRs) whenever more than $10,000 is brought into or out of the United States and are required to file reports of foreign bank and financial accounts (FBARs) whenever more than $10,000 is held in a foreign account in any given tax year. CTRs must be filed on any transaction exceeding $10,000 in a single business day.[90] CTRs must be filed within 15 days following the day on which the reportable transactions occurred.[91] Financial institutions must verify and record the name and address of the individual who conducted the reportable transactions and must accurately record the identity, social security number, or taxpayer identification number of any person or entity on whose behalf the reportable transaction was conducted.[92] CTRs are filed with FinCEN and are made available to law enforcement.

SARs must be filed on a variety of transactions, including those believed to be involved in money laundering or other illegal activity.[93] For MSBs, which, as described below, is the category most cryptocurrency exchangers and administrators fall within, SARs must be filed on transactions aggregating to at least $2,000 in value and the MSB knows or has reason to suspect (1) the funds were derived from illegal activity or were intended to hide or disguise funds or assets derived from illegal activity to violate or evade any federal law or regulation; (2) the transaction was designed to evade the Title 31 reporting requirements; (3) the transaction serves no business or apparent lawful purpose, and there is no other reasonable explanation for the transaction; and (4) the transaction involved the use of the money transmitter to facilitate criminal activity.[94] MSBs are required to file a SAR within 30 calendar days after detecting the underlying facts that warrant filing a SAR.[95] Lastly, MSBs are required to maintain supporting documentation for a SAR for five years from the

---

[90] *See* 31 C.F.R. §§ 1022.300, 1022.310, 1022.311, 1022.312 (cross-referencing 31 C.F.R. §§ 1010.300, 1010.310, and 1010.311, and 1010.312); *see also* 31 U.S.C. § 5313(a).

[91] 31 C.F.R. § 1010.306(a)(1).

[92] 31 C.F.R. § 1010.312.

[93] *See* 31 C.F.R. § 1010.320.

[94] 31 C.F.R. § 1022.320(a)(2).

[95] 31 C.F.R. § 1022.320(b)(3).

filing date, and these records must be made available to FinCEN or law enforcement upon request.[96]

The importance of SARs and CTRs to the integrity of the U.S. financial system cannot be overstated, as they are the lifeblood of most money laundering investigations. As such, failing to file a SAR or CTR is a federal crime.[97] Similarly, it is a crime for individuals to manipulate their transactions to prevent financial institutions from filing CTRs (called *structuring*), or to provide false information to financial institutions when making transactions that trigger the CTR filing requirement.[98] Ingeniously, the BSA also requires SARs to be filed on structuring activity, making criminals pick their poison of CTR or SAR.

In addition to filing these mandated reports, financial institutions are also obligated under the BSA to maintain an effective AML compliance program. Part of maintaining an effective AML program is filing SARs and CTRs.[99] The program must have written policies, procedures, and controls governing the verification of customer identification, the filing of reports such as CTRs, the creation and retention of records, responses to law enforcement requests, and other compliance with BSA requirements. The AML program must also have a designated compliance officer who is responsible for ensuring that the business complies with all BSA requirements. It is a federal crime under Title 31 for a financial institution to fail to maintain an AML program.[100]

B. Money transmitting under the BSA

A *financial institution* under the BSA includes much more than banks. Within the umbrella of financial institutions are MSBs.[101] Under the umbrella of MSBs are businesses involved in the transmission of funds, that is, money transmitters.[102] It should be noted that, while the Code of Federal Regulations uses the term *money transmitter*, Titles 31 and 18 use the term *money transmitting*

---

[96] 31 C.F.R. § 1022.320(c).
[97] 31 U.S.C. §§ 5313(a), 5322.
[98] 31 U.S.C. § 5324(a)(1), (3).
[99] 31 U.S.C. § 5318(h)(1); *see also* 31 C.F.R. § 1010.210.
[100] See 31 U.S.C. §§ 5318(h)(1), 5322.
[101] *See* 31 C.F.R. § 1010.100(t)(3).
[102] 31 C.F.R. § 1010.100(ff)(5).

business.[103] In addition to the regulatory definitions, Title 31 itself defines a financial institution as, among other things, "a licensed sender of money or any other person who engages as a business in the transmission of funds."[104]

Money transmitting is defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[105] Any means is defined as including electronic funds transfer or informal value transfers.[106] As such, a money transmitter can include an individual involved solely in the transmission of convertible virtual currencies.[107]

Federal regulations also exempt several categories of business and services from the definition of money transmitter, including communication service providers, payment processors, physical currency transporters, prepaid access card providers, and individuals who transmit funds integral to the sale of goods or the provision of services. [108] None of these exemptions apply to an individual involved in the exchange or transfer of cryptocurrency as a business. In May 2019, FinCEN issued guidance addressing how FinCEN regulations relating to MSBs apply to various business models involving money transmission denominated in cryptocurrencies, referred to in the guidance as convertible virtual currency or "CVC."[109] The guidance discussed the application of the BSA to foreign-located MSBs, individual P2P exchangers, wallet providers, cryptocurrency kiosk operators, CVC-to-CVC transactions, payment processors, mixers and tumblers, initial coin offerings, internet casinos, trading platforms, decentralized exchanges and distributed applications (DApps), miners, software providers, and developers of such technologies. The

---

[103] 18 U.S.C. § 1960; 31 U.S.C. § 5330.

[104] 31 U.S.C. § 5312(a)(2)(R).

[105] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[106] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[107] Guidance, Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [hereinafter, FinCEN 2013 Guidance].

[108] 31 C.F.R. § 1010.100(ff)(5)(ii); *see also* 31 C.F.R. § 1010.100(ff)(8)(iii) (natural persons engaged in activity on an infrequent basis and not for gain or profit are also exempted).

[109] 2019 Guidance, *supra* note 54.

guidance also detailed the application of FinCEN's regulations to persons who provide anonymizing services or who are engaged in activities involving anonymity-enhanced CVCs. According to FinCEN, anonymizing service providers and some AEC issuers are money transmitters, whereas an individual or entity that merely provides anonymizing software is not.

C. The Money Laundering Control Act

The federal money laundering violations are codified at 18 U.S.C §§ 1956, 1957, and 1960, and national security related money laundering violations can be found at 18 U.S.C §§ 2339(A)–(C).[110] Money laundering occurs when an individual knowingly conducts a financial transaction connected to, or stemming from, a criminal offense to promote the offense, conceal the proceeds, or evade federal reporting requirements. Depending on the facts and circumstances, transactions involving cryptocurrency can form the basis of concealment, promotion, sting, and international money laundering violations.[111]

1. The cases

Interestingly, it was a civil enforcement action by the Securities and Exchange Commission (SEC) that laid the groundwork in the courts for cryptocurrency transactions as *money* or *funds*. In the *Shavers* case, the SEC brought an action against Shavers for using bitcoin in a Ponzi-type investment scheme.[112] Shavers was later charged criminally in the Southern District of New York. The relevant ruling has been commonly relied upon in other federal money laundering cases involving cryptocurrency:

> It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and . . . used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for

---

[110] This article does not address the corresponding forfeiture statutes contained in the MLCA.

[111] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 21.

[112] Sec. Exch. Comm'n v. Shavers, No. 13-CV-416, 2013 WL 4028182 (E.D. Tex. 2013), *adhered to on reconsideration*, No. 13-CV-416, 2014 WL 12622292 (E.D. Tex. 2014).

> conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money . . .[113]

Following shortly thereafter, came the made-for-television prosecution of Ross Ulbricht, the administrator of the first dark web marketplace, Silk Road.[114] The U.S. Attorney's Office in the Southern District of New York filed a four-count indictment charging Ulbricht with numerous violations, including money laundering relating to his creation and administration of Silk Road. Ulbricht filed a motion to dismiss on a number of bases and contended that bitcoin transactions do not fall within the category of *financial transactions* covered by the money laundering laws. The district judge disagreed and denied Ulbricht's motion to dismiss in a detailed order, holding that "[o]ne can money launder using Bitcoin."[115]

Subsequent challenges to money laundering prosecutions involving cryptocurrency transactions have met similar fates.[116] In addition, three U.S. Circuit Courts have opined on cryptocurrency transactions as financial transactions supporting money laundering convictions.[117]

---

[113] *Id*. at *2.

[114] United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (denying a motion to dismiss money laundering charges). Ulbricht, known by the online moniker "Dread Pirate Roberts", was convicted following trial and sentenced to life imprisonment. The Second Circuit Court of Appeals affirmed his conviction and sentence. United States v. Ulbricht, 748 F. App'x 430 (2d Cir. 2019) (not precedential). The colorful story of Ulbricht and the Silk Road investigation and prosecution is detailed in the book *American Kingpin*. NICK BILTON, AMERICAN KINGPIN: THE EPIC HUNT FOR THE CRIMINAL MASTERMIND BEHIND THE SILK ROAD (2017).

[115] *Ulbricht*, 31 F. Supp. 3d at *24.

[116] *See* United States v. Ologeanu, 18-CR-81, 2020 WL 1676802 (E.D. Ky. Apr. 4, 2020) (denying Motion to Dismiss 1956 charges); United States v. Murgio, 209 F. Supp. 3d 698 (S.D.N.Y. 2016) (denying motions to dismiss and finding that bitcoins are funds); United States v. Faiella, 39 F. Supp. 3d 544 (S.D.N.Y. 2014) (denying motion to dismiss and finding that "[b]itcoin clearly qualifies as "money' or 'funds'").

[117] *See* United States v. Decker, 832 F. App'x 639 (11th Cir. 2020) (not precedential) (holding that the defendant's bitcoin transactions were financial transactions designed to conceal his drug trafficking activities); United States v. Costanzo, 956 F.3d 1088 (9th Cir. 2020) (stating that Bitcoin transactions affect interstate commerce for purposes of money laundering conviction); United States v. Lord, No. 15-00240-01/02, 2017 WL 1424806

D. Operating an unlicensed MSB: 18 U.S.C. § 1960

The statutory language of section 1960, coupled with FinCEN's March 2013 and May 2019 Guidance on the applicability of CVC to money transmitting regulations, clearly places many cryptocurrency-related activities and business models within the purview of the statute. As discussed above, the Bank Secrecy Act and its implementing regulations require MSBs to register with FinCEN by filing a registration of money services business (RMSB) and to renew the registration every two years.[118] Federal law also criminalizes the operation of a MSB without the appropriate registration.[119] This is a requirement separate and apart from state registrations, if any, that may be required by law. Section 1960 also criminalizes operating a MSB in violation of those state requirements.[120] Title 18, United States Code, section 1960(b)(1)(C) also criminalizes operating a MSB involved in the transport or transmission of funds known to the transmitter to have been derived from a criminal offense or that were intended to be used to promote and support unlawful activity.

E. FinCEN guidance and regulations

In March 2013, FinCEN released guidance about the requirement of certain participants in the virtual currency arena (which includes cryptocurrency such as bitcoin) to register as a MSB with the Department of the Treasury. The guidance defines three categories of participants in the virtual currency ecosystem: *exchangers*, *administrators*, and *users*. It defines an exchanger as a person or entity "engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency," and states that an exchanger who (1) accepts and transmits a convertible virtual currency; or (2) buys or sells convertible virtual currency for any reason *is* a money transmitter under FinCEN's regulations, unless a limitation to, or exemption from, the definition applies to the person.

(W.D. La. 2017), *aff'd*, 915 F.3d 1009 (5th Cir. 2019) (acknowledging bitcoin transactions in ML prosecution but appeal on other grounds).

[118] 31 U.S.C. § 5330; 31 C.F.R. § 1022.380.

[119] 18 U.S.C. § 1960(b)(1)(B).

[120] 18 U.S.C. § 1960(b)(1)(A).

Whether a person is a money transmitter is a matter of facts and circumstances.[121]

The regulations define the term *money transmitter* as a person that provides money transmission services, or any other person engaged in the transfer of funds; the term *money transmission services* means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[122] This language "transmission . . . to another location or person," was the basis of a number of legal challenges to section 1960 prosecutions in this context, but as further discussed in the cases below, district courts have held that transfers of cryptocurrency between addresses satisfy this definition.

The guidance, as clarified by an October 2014 request for administrative ruling,[123] defines a *user* as a person that obtains virtual currency to purchase goods or services on the user's own behalf and makes clear that "a user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is *not* an MSB under FinCEN's regulations." [124]

Further, 18 U.S.C. § 1960(b)(2s) defines *money transmitting* to include transferring funds on behalf of the public by any and all means. In May 2019, FinCEN issued interpretive guidance regarding the applicability of the Bank Secrecy Act and FinCEN regulations to certain business models.[125] This guidance serves as a helpful consolidation of FinCEN's prior guidance and related administrative rulings and application discussion to various virtual currency business models.

Importantly, the FinCEN registration requirements contained in section 1960(b)(1)(A) and (B) and the Bank Secrecy Act obligations are not mutually exclusive. A MSB's failure to register with FinCEN does not relieve the MSB of its obligations under the Bank Secrecy Act and implementing regulations. Nor does a MSB's registration with

---

[121] FinCEN 2013 Guidance, *supra* note 106.

[122] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[123] Response to Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform (Oct. 27, 2014) (FIN-2014-R011).

[124] FinCEN 2013 Guidance, *supra* note 64.

[125] Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019) (FIN-2019-G001).

FinCEN mean that the MSB fulfilled its requirements under the Bank Secrecy Act and regulations. In other words, a MSB might have complied with the Bank Secrecy Act and implementing regulations but failed to register as a MSB with FinCEN. Likewise, an entity might have registered as a MSB with FinCEN but not have complied with the Bank Secrecy Act and implementing regulations. Much like the drunk driver who denies liability because he does not have a driver's license, an unregistered MSB would be mistaken in assuming that it was not required to comply with the Bank Secrecy Act's anti-money laundering program and reporting requirements by virtue of the fact that it was not registered with FinCEN.

1. The cases

United States v. Harmon is a significant and recent case in the ever-developing area of cryptocurrency as a money laundering tool.[126] In *Harmon*, the District of Columbia District Court denied Harmon's motion to dismiss indictment counts two and three (which charged Harmon with operating Helix, an underground tumbler for bitcoins on the Darknet), holding that bitcoins are money under the District of Columbia's Money Transmitter's Act (MTA) and that Helix was sufficiently alleged to be an unlicensed money transmitting business under section 1960(b)(1)(B).[127] The *Harmon* court found that bitcoins fall under "the ordinary definition of money," which means "a medium of exchange, method of payment, or store of value," and that bitcoins qualify as money under the MTA.[128] The court held that the government sufficiently alleged that Harmon's bitcoin tumbler qualified as an "unlicensed money transmitting business" under 18 U.S.C. § 1960(b)(1)(B) because the tumbler moved funds from one person or place to another.[129] The opinion also provides an excellent primer on bitcoins and the Darknet.

Harmon is preceded by a line of cases across numerous district courts denying motions to dismiss section 1960 charges brought against bitcoin exchangers.[130]

---

[126] United States v. Harmon, No. 19-395, 2020 WL 4251347 (D.D.C. July 24, 2020).

[127] *Id*. at *22.

[128] *Id*. at *7–*8.

[129] *Id*. at *22.

[130] *See* Opinion & Order, United States v. Green, No. 19-cr-525 (D.N.J. Feb. 10, 2020), ECF No. 30 (denying motion to dismiss 1960 charges against

Despite the fact that they are not binding on any U.S. district court and have been overruled and reversed respectively, two cases, *Petix* and *Espinoza*, are worth noting as often cited authority in support of motions to dismiss section 1960 prosecutions against cryptocurrency money transmitters, namely P2P exchangers. In *United States v. Petix*, the defendant, on federal supervision following his conviction for transporting child pornography, was detected by U.S. Probation using computers in violation of his supervised release conditions.[131] Investigators determined that the defendant advertised buying and selling bitcoin on a known cryptocurrency exchange platform and was subsequently caught conducting a bitcoin transaction worth $13,000 at a local coffee shop using an unauthorized computer and other electronic devices. The U.S. Attorney's Office charged him with violating section 1960. The defendant filed a motion to dismiss, and the district judge referred it to the magistrate for a report and recommendation (R&R). The U.S. Magistrate recommended granting the motion to dismiss, finding that "[b]ecause Bitcoin does not fit an ordinary understanding of the term 'money,' Petix cannot have violated Section 1960 in its current form," and agreeing with a Florida state money transmitter case, *Espinoza*, which granted a similar motion to dismiss.[132] Prosecutors filed objections to the R&R, and after hearing argument on the issue, the district judge announced on the record that he would not adopt the magistrate's findings and

---

bitcoin exchanger); United States v. Stetkiw, No. 18-20579, 2019 WL 417404 (E.D. Mich. Feb. 1, 2019) (denying motion to dismiss in 1960 prosecution against bitcoin exchanger); United States v. Mansy, No. 15-CR-198, 2017 WL 9672554 (D. Me. 2017) (denying motion to dismiss in 1960 prosecution against bitcoin exchanger); United States v. Murgio, 209 F. Supp. 3d 698 (S.D.N.Y. 2016) (motions to dismiss and finding that bitcoins are funds within the meaning of section1960 and IRS designation of bitcoins as property is irrelevant to the charges); United States v. Faiella, 39 F. Supp. 3d 544 (S.D.N.Y. 2014) (denying motion to dismiss and citing the FinCEN guidance and Title 31 in support of finding that the defendant was a "money transmitter" and did not fall under the exemption of being involved in the sale of goods or provision of services).

[131] United States v. Petix, No. 15-cr-00227, 2016 WL 7017919 (W.D.N.Y. 2016).

[132] *Id.* at *1.

allowed the defendant to withdraw his motion to dismiss.[133] Shortly thereafter, the defendant entered a guilty plea.

In the *Espinoza* case mentioned above, the defendant was charged under Florida state statutes (state equivalents to sections 1956 and 1960) with unauthorized money transmission and money laundering following a sting operation where government agents bought bitcoin for cash from the defendant seller advertising on a bitcoin P2P exchange platform.[134] The defendant filed a motion to dismiss, and the judge granted the motion, finding that the defendant was selling his personal property, not transmitting from one person or place to another; he didn't charge a fee for the transaction (although he did make a profit); bitcoin "cannot be hidden under a mattress like cash and gold bars;" and that bitcoins are not monetary instruments that can be used as the basis of a money laundering financial transaction. Moreover, the court completely disregarded several factually similar rulings from the U.S. District Court for the Southern District of New York.[135] On appeal, the Florida Appellate Court in Miami reversed the dismissal order and held that selling bitcoin constitutes money transmission under Florida's money transmitter law.

VII. Looking ahead: preparing for the second and third waves

Because the cryptocurrency global ecosystem is evolving at such a rapid pace, it is worth noting recent developments affecting blockchain-based technologies and business models, as well as law enforcement's ability to obtain necessary evidence and recover virtual assets involved in money laundering.

---

[133] The District Judge did not enter a written opinion overruling the Magistrate's Report and Recommendation; however, a review of the docket sheet clearly indicates that the Report and Recommendation was not adopted, and the court allowed the defendant to withdraw his motion before pleading guilty.

[134] Florida v. Espinoza, No. F14-293 (Fla. Cir. Ct. July 22, 2016), *rev'd* State v. Espinoza, 264 So.3d 1055 (Fla. 3rd Dist. Ct. App. 2019); *see also* United States v. Murgio, 209 F. Supp. 3d 698 (S.D.N.Y. 2016) (disagreeing with legal findings in Espinoza).

[135] *See* United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014); *Murgio*, 209 F. Supp. 3d 698; *Faiella*, 39 F. Supp. 3d 544.

A. The Financial Action Task Force

As a standard-setting and policy-making body, the Financial Action Task Force (FATF) works to generate the technical understanding and necessary political will to bring about national legislative and regulatory reforms, which are intended to be harmonized across jurisdictions to the greatest extent possible. The FATF accomplishes this goal by developing a series of "recommendations" that are recognized as the international standards for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. Countries, however, are responsible for devising and implementing the standards for compliance by the private sector entities operating in their jurisdictions. Why does this matter? In a 2020 podcast, blockchain-regulation guru Siân Jones put it wisely, "FATF recommendations are not merely recommendations; they are recommendations with serious economic consequences for countries that fail to adopt and implement them."[136]

Thus, adopting regulations and providing supervision in line with these recent virtual asset-related recommendations will deter exchanges and other regulated service providers located abroad from allowing or turning a blind eye to cryptocurrency used for illicit purposes, including money laundering, on their platforms. In addition, as countries implement and enforce these regulations, virtual asset service providers, wherever they are located, will have record keeping and reporting requirements equivalent to traditional fiat financial institutions, resulting in a more transparent flow of funds in cryptocurrency transactions that touch these service providers and an increased access to important evidence by investigators globally.

B. Decentralized Finance (DeFi)

Decentralized Finance (DeFi) collectively refers to blockchain-based financial products and services, to include token lending and trading. DeFi removes centralized entities and enables users to pseudonymously transfer funds in minutes.[137] As of December 2020,

---

[136] *See* Laura Shin, W*hy the Travel Rule is One of the Most Significant Regulations in Crypto*, UNCHAINED (Aug. 4, 2020), https://unchainedpodcast.com/why-the-travel-rule-is-one-of-the-most-significant-regulations-in-crypto/.

[137] *Decentralized Finance (DeFi)*, ETHEREUM, https://ethereum.org/en/defi/ (last visited May 10, 2021).

$14.2 billion was held in DeFi technologies, according to DeFi Pulse, a website that monitors the open source Ethereum blockchain.[138] Additionally, decentralized exchange (DEX) trading volume skyrocketed from under $1 billion dollars in transactions in January 2020 to well over $25 billion in September 2020.[139]

Just one example of a DeFi product is Maker, a set of smart contracts that mints the stablecoin Dai. According to its website, the Maker Protocol was the first DeFi application to earn significant adoption and is one of the largest on the Ethereum blockchain.[140]

C. Decentralized exchanges (DEXs)

DEXs are software that operate as an exchange, enabling individuals to exchange with other traders directly, on a P2P basis, without needing to trust an intermediary or each other.[141] As a result, there is no centralized entity, raising questions about responsible parties for legal compliance. Rather, the technology replaces the role that a centralized exchange plays in a traditional virtual asset transaction; therefore, there may be no identifiable entity for service of legal process. Using DEXs, criminals can instantly exchange virtual assets anonymously worldwide with little to no concern for customer due diligence procedures or seizure by law enforcement.

DEXs automatically pair users wishing to trade virtual assets. When DEXs pair users who trade one virtual asset for another on another blockchain, this is called a "cross-chain atomic swap."[142] While DEXs do not allow for the trading of all virtual assets (the asset must be listed on the exchange), these types of trades allow for

---

[138] DeFi Pulse, https://defipulse.com. "DiFi Pulse monitors each protocol's underlying smart contracts on the [openly viewable Ethereum] blockchain . . . [and] pull[s] the total balance of Ether (ETH) and . . . tokens held by those smart contracts." DeFi Pulse calculates the total value locked amount by multiplying those balances by their price in U.S. dollars. *Id.*

[139] *Dex Tracker—Decentralized Exchanges Trading Volume*, DEF BLOG, https://defiprime.com/dex-volume (last visited May. 10, 2021).

[140] *Learn About MakerDAO*, MAKERDAO, https://community-development.makerdao.com/en/learn/MakerDAO (last visited May 10, 2021).

[141] Will Warren, *Decentralized Exchange*, COIN CENTER (Oct. 10, 2018), https://www.coincenter.org/education/key-concepts/decentralized-exchange/.

[142] *Id.*

trustless exchanges of cryptocurrencies that exist on distinct and different blockchains.[143]

In addition to individual DEXs, trades on these platforms may be conducted through third-party services, traditionally referred to as *aggregators*.[144] Aggregators sync with numerous DEXs to facilitate trades in an automated fashion, pulling data from multiple DEXs' order books to provide customers the best pricing options for their trade.[145] These services can provide an additional automated layer of anonymity for criminals laundering illicit funds by not trading directly with the underlying DEX. But even with the growing use of DEXs, criminals will still need to use traditional financial institutions to cash out their cryptocurrencies.

DEX case study: Kucoin hack

In September 2020, approximately $281 million in virtual assets was stolen from Kucoin, a Singapore-based exchange. According to open source reports, the blockchain forensics company Elliptic traced over $17 million of the stolen funds to DEXs and DEX aggregators. [146]

---

[143] *Id.*

[144] Joshua Iversen, *Top 5 DEX Aggregators, Rated & Reviewed for 2021*, BITCOIN MKT. J. (Jan. 6, 2021), https://www.bitcoinmarketjournal.com/top-dex-aggregators; Mary Thibodeau, *What are DEX Aggregators in Crypto Markets*, HEDGETRADE (Feb. 14, 2020), https://hedgetrade.com/what-are-dex-aggregators/.

[145] Thibodeau, *supra* note 143.

[146] Terence Zimwara, *Kucoin Hack: $17M Laundered Via Decentralized Exchanges, Blockchain Analysis Firm Claims This Can Still be Traced*, BITCOIN (Oct. 2, 2020), https://news.bitcoin.com/kucoin-hack-17m-laundered-via-decentralized-exchanges-blockchain-analysis-firm-claims-this-can-still-be-traced/.

D. Flash lending

Another popular use of DeFi involves flash lending. Flash lending uses smart contracts to enable a user to take out an instant, uncollateralized loan, use the loan, and repay the loan—all in the same transaction. This functionality might be used for a variety of purposes, to include arbitrage, wash trading, or collateral swapping.

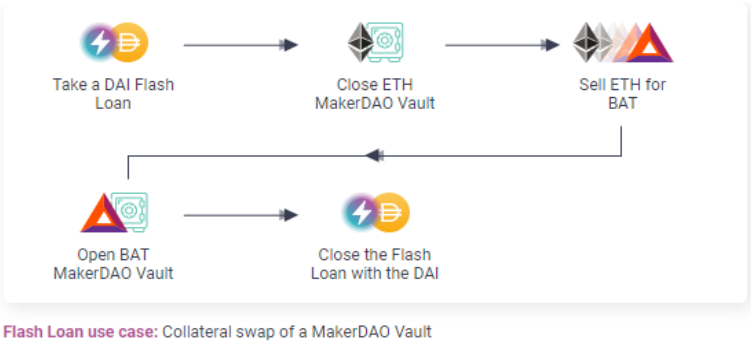


Figure 4: Flash Loan Use Case Example[147]

Between December 2019 and December 2020, DeFi lending grew 1,288%, from $451.6 million to $6.27 billion according to DeFi Pulse, a website that publishes data related to the Ethereum blockchain.[148] In July 2020, DeFi loan protocol Aave saw more than 1,000% growth, from $11 million to more than $130 million, in the daily value of flash loans issued, according to Cointelegraph.[149] In February 2020, two separate illicit actors exploited the rapid and complex flash loan process to obtain a total of $954,000 through an instantaneous "pump and dump" scheme.[150]

---

[147] *Flash Loans: Pushing the Limits of DeFi*, AAVE https://aave.com/flash-loans/ (last visited May 10, 2021); *see also Vaults*, MAKERDAO, https://community-development.makerdao.com/en/learn/vaults (last visited May 10, 2020).

[148] DEFI PULSE, https://defipulse.com (last visited May 10, 2020).

[149] Samuel Haig, *Aave Ascends Market Rankings as Flash Loans Explode*, COINTELEGRAPH (July 29, 2020), https://cointelegraph.com/news/aave-ascends-market-rankings-as-flash-loans-explode. Cointelegraph is a virtual asset news online publication. In part, Cointelegraph cites data from DiFi Pulse.

[150] Will Heasman, *5Are the BZx Flash Loan Attacks Signaling the End of DeFi*, COINTELEGRAPH (Feb. 22, 2020), https://cointelegraph.com/news/are-

Thus, the increased use and the nature of these DeFi platforms, whether in the form of a DEX or decentralized application offering flash loans, may pose money laundering risks going forward. The lack of human intervention in these DeFi platforms is likely appealing to criminals and may cause DeFi to play a bigger role in crypto-laundering in the future.[151]

E. Central Bank Digital Currencies (CBDCs)

Central Bank Digital Currencies (CBDCs) may use blockchain-based tokens to represent a nation state's official fiat currency.[152] According to the FATF, CBDC are not virtual assets but digital representations of fiat currency with unique characteristics.[153] For example, as a CBDC, the Chinese yuan becomes the "digital yuan." In contrast to decentralized cryptocurrencies like Bitcoin or Ether, CBDCs are centralized, issued, and regulated by the competent monetary authority of the country.[154] Depending on the ultimate implementation of the technology, CBDCs could become a favored medium for illicit activities, in part due to benefits related to ease of use and transaction velocity.

In 2017, the Russian government announced its intention to create its own CBDC, the "crypto-ruble." According to one of Vladimir Putin's economic advisers, "This instrument [the crypto-ruble] suits us very well for sensitive activity on behalf of the state. We can settle accounts with our counterparties all over the world with no regard for sanctions."[155]

---

the-bzx-flash-loan-attacks-signaling-the-end-of-defi. Cointelegraph cites a bZx post-mortem relating to one incident and other public posts from the company.

[151] *See* THE 2021 CRYPTO CRIME , *supra* note 17, at 107–08.

[152] Alyssa Hertig, *What is a CBDC?*, COINDESK (Dec. 22, 2020), https://www.coindesk.com/what-is-a-cbdc.

[153] FIN. ACTION TASK FORCE, FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS ON SO-CALLED STABLECOINS 26–27 (2020).

[154] Hertig, *supra* note 151.

[155] Max Seddon & Martin Arnold, *Putin Considers 'Cryptorouble' as Moscow Seeks to Evade Sanctions*, FIN. TIMES (Jan. 1, 2018), https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da. Financial Times is based in the United Kingdom, owned by a Japanese holding company, and reports on business and economic current affairs.

In 2020, various international bodies issued reports on CBDCs, documenting the status of projects, highlighting risks, and setting out standards for regulation and supervision of this technology. [156] As of January 2020, 80% of central banks were engaging in some intentional efforts to understand the implications of a CBDC for their jurisdictions, with 40% progressing from conceptual research to experiments or proof of concepts. [157]

In October 2020, the Bahamas officially launched the first CBDC available to all residents, known as the Sand Dollar. [158] While the Sand Dollar was introduced solely within Bahamian borders, many

---

[156] BANK OF CANADA ET AL., CENTRAL BANK DIGITAL CURRIENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES (2020). The Bank of International Settlements is owned by 63 central banks representing countries that, together, account for 95% of the world gross domestic product. The report was published by the Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve Bank, and Bank for International Settlements. FIN. STABILITY BD., REGULATION, SUPERVISION AND OVERSIGHT OF "GLOBAL STABLECOIN" ARRANGEMENTS (2020). The Financial Stability Board (FSB) coordinates, at the international level, the work of national financial authorities and international standard-setting bodies to develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities. FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS ON SO-CALLED STABLECOINS, *supra* note 152. The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

[157] CODRUTA BOAR ET AL., IMPENDING ARRIVAL—A SEQUEL TO THE SURVEY ON CENTRAL BANK DIGITAL CURRENCY (2020). The Bank of International Settlements is owned by 63 central banks representing countries that together account for 95% of the world gross domestic product. This paper surveyed 66 central banks, 21 from advanced economies and 45 from emerging market economies.

[158] Vipin Bharathan, *Central Bank Digital Currency: The First Nationwide CBDC In the World Has Been Launched by the Bahamas*, GALAXY (Oct. 21, 2020), https://www.forbes.com/sites/vipinbharathan/2020/10/21/central-bank-digital-currency-the-first-nationwide-cbdc-in-the-world-has-been-launched-by-the-bahamas/?sh=44fc5094506e.

other countries are piloting or developing CBDCs of their own for widespread use.[159] China's CBDC pilot processed over 4 million transactions, totaling over 2 billion yuan ($299 million) in the digital currency between April and November 2020.[160] For a discussion of the national security implications of China's development of its CBDC system, the authors suggest reading the Center for New American Security's (CNAS) recent report on the topic.[161]

What is the U.S. stance on issuance of a U.S. dollar-backed CBDC? In 2020, the Federal Reserve Bank of Boston and researchers at the Massachusetts Institute of Technology's Digital Currency Initiative announced a multiyear collaboration to investigate how to build a CBDC with the necessary features to be a new form of currency for the U.S. economy.[162] Called "Project Hamilton," the initiative uses existing and new technologies to build and test a hypothetical digital currency platform.[163]

As countries develop and circulate CBDCs globally, it will be interesting to monitor how and to what extent these financial technologies may be used to launder money. Whether these digital fiat currencies will produce a monsoon or simply lap along the shore alongside established financial products remains to be seen. One thing seems fairly certain: Blockchain-based financial technologies are here

---

[159] Hertig, *supra* note 151.

[160] Jonathan Cheng, *China Rolls Out Pilot Test of Digital Currency*, WALL ST. J. (Apr. 20, 2020), https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339. The Wall Street Journal cited official comment from the People's Bank of China and screenshots from the digital currency wallet application that circulated on the Internet. *PBOC Governor Says 4 Million Transactions so Far in Digital Yuan*, BNN BLOOMBERG (Nov. 1, 2020), https://www.bnnbloomberg.ca/pboc-governor-says-4-million-transactions-so-far-in-digital-yuan-1.1516222.

[161] YAYA FANUSIE & EMILY JIN, CHINA'S DIGITAL CURRENCY: ADDING FINANCIAL DATA TO DIGITAL AUTHORITARIANISM (2021).

[162] Treacy Reynolds, *The Federal Reserve Bank of Boston Announces Collaboration With MIT to Research Digital Currency*, FED. RSRV. BANK OF BOSTON (Aug. 13, 2020), https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx.

[163] Jim S. Cunha, *Boston Fed's Digital Dollar Research Project Honors 2 Hamiltons, Alexander and Margaret*, FED. RSRV. BANK OF BOSTON (Feb. 25, 2021), https://www.bostonfed.org/news-and-events/news/2021/02/how-did-the-feds-digital-dollar-project-get-its-name-project-hamilton.aspx.

to stay. Thus, investigators, prosecutors, and financial institutions with AML obligations need to get onboard or risk drowning in the under current.

About the Authors

Alexandra D. Comolli is a Management and Program Analyst in the Federal Bureau of Investigation's Criminal Investigative Division, where she specializes in the investigation of virtual currency money laundering and money laundering facilitation matters across threats programs. She also covered transnational criminal organizations operating on the Darknet and supported the FBI's international efforts to combat cybercrime. She is a graduate of Duke University and the Antonin Scalia Law School at George Mason University and is admitted to the Massachusetts bar.

Michele R. Korver is the Digital Currency Counsel in the Criminal Division's Money Laundering and Asset Recovery Section, serving as a subject-matter expert for the Department on prosecutions and forfeitures involving cryptocurrency. Michele has served as an Assistant United States Attorney in the Miami, Florida, and Denver, Colorado, United States Attorney's Offices, where she investigated and prosecuted hundreds of violations of federal criminal law in U.S. courts. Michele started her career as a Special Agent with the U.S. Secret Service and clerked for the Honorable William P. Dimitrouleas in the U.S. District Court for the Southern District of Florida.

Note from the Editor-in-Chief

The Department of Justice's Office of Legal Education is proud to present the Technology & Law issue of the DOJ Journal of Federal Law and Practice. As we move further into the twenty-first century, attorneys who practice criminal law must become acquainted with the latest in technology, lest they be left back in the days of adding machines, carbon paper, and the telegraph. This issue has it all, including discussions about smartphones, cryptocurrency, and drones. In addition, there are important articles on electronic investigative techniques, search warrants, and filter teams. If you were looking for the latest on high tech, you've come to the right place.

With this issue, we say goodbye to Associate Editor Gurbani Saini. Gurbani has been with the OLE Publications Team for over three years, starting as a clerk while she attended the University of South Carolina School of Law. After graduation, she took a permanent position as a USC independent contractor. In that role, she was a beloved member of "Pubs," coordinating article submissions with authors, managing needs assessments for OLE blue books, and editing manuscripts. Through it all, Gurbani was always upbeat and a joy to have as a colleague. She never seemed to have a bad day—or if she did, you never knew it. (And that includes the day she and I had to figure out a Bluebook citation form for a French treaty.) We will miss her but wish her well in her future endeavors.

As always, we couldn't produce this law review without help. Kudos go out to Puneet V. Kakkar and Joseph Wheatley who acted as points of contact for this issue and recruited our authors. Thanks also to Managing Editor Addison Gantt, Associate Editors Gurbani Saini and Philip Schneider, and our law clerks. But most of all, thanks to our readers, both inside and outside of the Department, who inspire us to greater heights.

Chris Fisanick
Columbia, South Carolina
May 2021