2024 WL 860983
Only the Westlaw citation is currently available.
United States District Court, District of Columbia.

UNITED STATES of America,

v.

Roman STERLINGOV, Defendant.

Criminal Action No. 21-399 (RDM)
|
Signed February 29, 2024

Synopsis

Background: Defendant was charged with money laundering, money laundering conspiracy, operating unlicensed money transmitting business, and money transmission without license. Defendant moved to exclude government's blockchain tracing evidence.

Holdings: The District Court, Randolph D. Moss, J., held that:

government demonstrated by preponderance of evidence that blockchain tracing analysis generated by proprietary computer software program was product of reliable principles and methods;

proprietary computer software program that clustered hundreds of thousands of addresses to gauge magnitude of illicit activity could be and had been tested;

co-spend heuristic in that software had widespread academic approval;

lack of compiled "error rate" for that software did not diminish its reliability; and

both law enforcement and business communities had widely relied upon blockchain tracing, like software at issue, supporting use of program by expert when testifying.

Motion denied.

Attorneys and Law Firms

Jeffrey Pearlman, Catherine Pelker, Assistant U.S. Attorneys, U.S. Department of Justice, Washington, DC, Christopher Brodie Brown, Assistant U.S. Attorney, DOJ-USAO, Washington, DC, for United States of America.

Tor Ekeland, Pro Hac Vice, Tor Ekeland Law PLLC, Brooklyn, NY, Marina Medvin, Medvin Law PLC, Alexandria, VA, Michael Hassard, Pro Hac Vice, Tor Ekeland Law PLLC, New York, NY, for Defendant.

MEMORANDUM OPINION AND ORDER

RANDOLPH D. MOSS, United States District Judge

***1** Defendant Roman Sterlingov is charged with money laundering conspiracy, money laundering, operating an unlicensed money transmitting business, and money transmission without a license, all in relation to his alleged operation of a bitcoin mixer known as Bitcoin Fog. Dkt. 43 (Superseding Indictment). Both sides have proffered multiple expert witnesses. In June, July, and August 2023, the Court held a series of *Daubert* hearings at which it heard testimony from nearly all of these proposed experts and considered lengthy expert reports, at least one of which was accompanied by a series of large datafiles. *See, e.g.*, Dkt. 224 (June 23, 2023 Hrg. Tr.); Dkt. 228 (Aug. 22, 2023 Hrg. Tr.); Dkt. 229 (Aug. 23, 2023 Hrg. Tr.). In September, the Court heard argument on the admissibility of the proposed experts' testimony. *See* Dkt. 232 (Sept. 7, 2023 Hrg. Tr.); Dkt. 233 (Sept. 8, 2023 Hrg. Tr.); Dkt. 235 (Sept. 15, 2023 Hrg. Tr.); Dkt. 236 (Sept. 18, 2023 Hrg. Tr.). The parties subsequently submitted supplemental briefing concerning a subset of the expert testimony issues, as well as further supporting evidence. Dkt. 191; Dkt. 192; Dkt. 193. The Court has issued multiple rulings from the bench regarding the admissibility of the proposed expert testimony. This opinion provides additional explanation regarding the Court's rejection of defendant's *Daubert* challenge to the reliance by two of the government's experts, Luke Scholl of the Federal Bureau of Investigations ("FBI") and Elizabeth Bisbee of Chainalysis Government Solutions ("Chainalysis"),

on a software product known as Chainalysis Reactor ("Reactor").

Although bitcoin transactions are anonymous in the sense that each transaction is identified only by lengthy sets of numbers and letters representing the sending address(es), the receiving address(es), and the transaction ID(s), they are, at the same time, public in the sense that the amount, timing, sending address(es), and receiving address(es) of every transaction is recorded on the blockchain, which is a decentralized, immutable, public ledger available to anyone with an interest in looking. As result, bitcoin transactions are both uniquely anonymous and uniquely public. As explained further below, the public ledger permits law enforcement and others not only to trace bitcoin moving through specific transactions, but to cluster bitcoin addresses in a manner that provides a window into otherwise anonymous activity. The most widely accepted means of clustering relies on a concept referred to as "co-spend," which occurs when the user on the sending side of the transaction draws on bitcoin held in multiple addresses. It is possible to associate those multiple sending addresses with a single sender, since the sender would need the "private key," akin to a password, for each of the sending addresses to effectuate the transfer. When the process of identifying co-spend transactions is repeated for multiple transactions, it is possible to build a larger and larger cluster associated with the user or entity in question.

***2** Given the volume of transactions recorded on the blockchain, investigators frequently make use of proprietary software like Chainalysis Reactor to cluster bitcoin transactions using the co-spend and other heuristics. Much of this work could be done manually given enough time, and as explained below, it is possible to corroborate (or to challenge) the results generated by the software for particular clusters with the public blockchain data, a pad of paper, a pencil, and hours of work.[1] Reactor also uses other heuristics based on unique identifiers that Chainalysis has associated with particular services that have in the past or that currently transact on the blockchain.

[1] In one company's account: "Prior to selecting Reactor as its investigating solution, [the exchange] was doing the work manually, which was particularly challenging for investigating peel chains. With the new Peel Chain Detection feature in Reactor, the team can now automate much of that work with a single click." *Bitstamp Chooses Chainalysis to Supercharge Its Compliance Program*, Chainalysis, https://www.chainalysis.com/customer-story-bitstamp (last visited Feb. 28, 2024).

The defense argues that Scholl and Bisbee's reliance on Reactor fails the *Daubert* test and that the Court should, accordingly, exclude all testimony and evidence based on clustering performed using that software. The defense contends that Reactor is "junk science," which has not been peer reviewed and has no known error rate, and that, as a result, any testimony based on Reactor is not "the product of reliable principles and methods," Fed. R. Evid. 702(c). For the reasons explained below, the Court is unpersuaded. Although the defense is correct that not all of the heuristics used in this case have been subject to "peer review" and that Chainalysis does not gather and record an error rate in a central location, substantial evidence supports the government's submission that the software is highly reliable—and, if anything, conservative—in clustering (and then attributing) bitcoin addresses. The defense, of course, remains free to challenge the accuracy and reliability of Reactor before the jury. But the Court is satisfied that it is "more likely than not" that the evidence and testimony at issue will help the jury to understand the evidence, that it is based on sufficient facts or data and reliable principles and methods, and that Scholl and Bisbee have reliably applied those principles and methods. *See* Fed. R. Evid. 702.

I. BACKGROUND

A. The Bitcoin Blockchain

Some explanation of the Bitcoin system and the blockchain is necessary to understand how Reactor operates. "Bitcoin is a purely online virtual currency, unbacked by either physical commodities or sovereign obligation," and which, instead, "relies on a combination of cryptographic protection and peer-to-peer protocol for witnessing settlements." Sarah Meiklejohn *et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, at 1 (October

2013), https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (hereinafter "Meiklejohn"). Although other cryptocurrencies exist, Bitcoin is the most popular. Each unit of currency on the "Bitcoin" system (referred to with a capital B) is called a "bitcoin" (referred to with a lowercase b). *See United States v. Harmon*, 474 F. Supp. 3d 76, 80–81 (D.D.C. 2020).

The Bitcoin system is a peer-to-peer network "enabling proof and transfer of ownership" of bitcoin "without involving a third-party such as a bank," *id.* at 80, or any other central authority in its transaction. Bitcoin transactions are recorded on a decentralized, immutable, chronological, public ledger, referred to as the "blockchain." In simplified terms, transferring or using bitcoin requires three things: (1) a sending address, (2) a receiving address, and (3) a private encryption key. An address is a "long string of letters and numbers"—usually twenty-five characters or longer—and is similar to a bank account number. *Id.* at 81 (citing *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020)). Every address is associated with a public key, which is derived from a private key. Private keys "are secret, like passwords." *Id.* "[U]sers can use any number of public keys and their activity using one set of public keys is not inherently tied to their activity using another set, or to their real-world identity." Meiklejohn at 2. "[B]ecause each of these transactions references the previous transaction (i.e., in sending bitcoins, the current owner must specify where they came from), the transactions form a chain," and "[t]o verify the validity of a bitcoin, a user can check the validity of each of the signatures in this chain." *Id.*

***3** "To transfer bitcoin from one address to another, the sender transmits a message—called a transaction—on the Bitcoin public network, and that transaction is eventually recorded on a blockchain." *Harmon*, 474 F. Supp. 3d at 81. "The transaction must contain: (1) the amount of bitcoin to be transferred; (2) the address to which the bitcoin will be sent [the receiving address]; (3) the address from which the bitcoin is being sent [the sending address]; and (4) the public key associated with the sender and the sending address." *Id.* In order to execute the transaction, "the sender must sign the transaction using a digital signature generated using the sender's private key. Once signed, the transaction is broadcast to the Bitcoin network." *Id.* (internal citations omitted). To verify the transaction, the network confirms that:

> (1) the public key is associated with the address of the sender and (2) the digital signature was produced for this transaction using the sender's private key. After the transaction is verified, the bitcoin being sent becomes associated with the recipient address and its attendant private and public keys. The transaction is also recorded on the blockchain. The recording process is a complex one that involves nodes on the network "bundling up transactions into blocks of aggregated transactions and appending each block to the prior block."

Id. at 81–82 (internal citations omitted).

A transaction "generally incurs a 'common fee' or 'miner transaction fee' associated with this verification process." *United States v. Costanzo*, 956 F.3d 1088, 1091 (9th Cir. 2020). "Mining" is the process by which individuals contribute their computing power to solve a complex algorithm that is used to verify and to record payments on the blockchain using computers (referred to as "nodes") operating within the distributed system. In exchange for contributing their computing power, miners receive bitcoin. Once the miner verifies the transaction, "he broadcasts it to his peers, who again broadcast it to their peers." Meiklejohn at 3. Transaction fees can be used to incentivize miners to select or to prioritize certain transactions over others—typically, the higher the transaction fee offered, the more quickly a transaction is confirmed. *See* Eric D. Chason, *How Bitcoin Functions As Property Law*, 49 Seton Hall L. Rev. 129, 162–63 (2018). The final result of this process is that "every node in the network 'has a current, immutable history of all transactions ever logged on the blockchain.' " *Harmon*, 474 F. Supp. 3d at 81–82 (internal citations omitted).

As relevant here, the Bitcoin blockchain records "only the sender's address, the receiver's address, and the amount of Bitcoin transferred," *id.* at 82, along with a unique time stamp used to prevent double spending, Meiklejohn at 2. In this sense, the transaction is pseudonymous—but, at the same time, "all transactions are completely transparent." *Id.* at 1. Every transaction is recorded and publicly available on the ever-growing blockchain ledger. And, even though the "owners of addresses are anonymous," "it is possible to discover the owner of a Bitcoin address by

analyzing the blockchain." *Harmon*, 474 F. Supp. 3d at 82 (quoting *Gratkowski*, 964 F.3d at 309). Chainalysis and its peer blockchain analytics companies (including Ciphertrace by Mastercard, Elliptic, and TRM Labs) are in the business of analyzing the Bitcoin blockchain.

B. Chainalysis Reactor

Chainalysis Reactor is a software product used to cluster cryptocurrency addresses that are likely controlled by the same entity and to then tie those clusters to particular entities based on information gleaned from other sources, including by conducting test transactions with those entities, researching open sources, and exchanging information with various cryptocurrency exchanges and law enforcement agencies. *See* Bisbee Expert Report at 5. Here, Reactor clustered and attributed to Bitcoin Fog over 900,000 addresses, traced receipt of approximately 1,284,251 bitcoin (valued at almost $400 million) to Bitcoin Fog, and traced withdrawals of approximately 1,280,935 bitcoin (valued at a little over $400 million) from Bitcoin Fog. *Id.* at 9. Reactor also clustered and attributed thousands of Bitcoin addresses to eight darknet market sites, including AlphaBay Market, Evolution Market, Agora Market, and Pandora Market, and concluded that "[t]he eight darknet market services sent an aggregate direct amount" of about 80,729 bitcoin (valued at over $27.9 million) to Bitcoin Fog and received over 45,152 bitcoin (valued at over $14.5 million) directly from Bitcoin Fog between October 2013 and July 2017. *Id.* at 27. According to the results generated by Reactor, these same darknet market sites also *indirectly* sent to Bitcoin Fog and *indirectly* received from Bitcoin Fog many thousands of additional bitcoin, valued at many millions of dollars. *Id.*

***4** As explained by Bisbee and reflected in expert reports and discovery provided to the defense, Reactor clusters addresses using three "heuristics." *Id.* at 5. The term "heuristic" has long been used by the cryptography community to describe cryptocurrency clustering techniques. *See, e.g.*, Meiklejohn at 5 ("In this section, we present two heuristics for linking addresses controlled by the same user, with the goal of collapsing the many public keys seen in the block chain into larger entities."). As Bisbee explains, a heuristic is a "computational function that ranks different search algorithms at each branching step based on available information to decide which branch to follow." Bisbee Expert Report at 5 n.2.

Chainalysis uses three types of heuristics. First, it uses the co-spend or common spend heuristic, referred to as "Heuristic 1." This heuristic is based on a unique feature of the blockchain: "A transaction can contain multiple input addresses and multiple output addresses," and "[w]hen a transaction contains multiple inputs addresses, the input addresses are said to be co-spending." Scholl Expert Report at 4. But because each transaction input requires that the sender have access to the private key for each of the corresponding input addresses, it is very likely that a single person or entity controls each of the input addresses. *See id.* Imagine, for example, that a virtual wallet holds three bitcoin addresses. The first address contains 1.5 bitcoin, the second address contains 2 bitcoin, and the third address contains 3 bitcoin. If the owner of the wallet wants to purchase an item that costs 4.5 bitcoin, or transfer that amount to a different address for any other reason, he would need to fund that transaction with two of his three addresses. In order to do so, moreover, he would have to enter the private key for each sending address. Using the co-spend heuristic, it would then be possible to cluster the two co-spending input addresses together because it is highly unlikely that a user would share his private keys with others. The following diagram reflects this simplified example of co-spending:

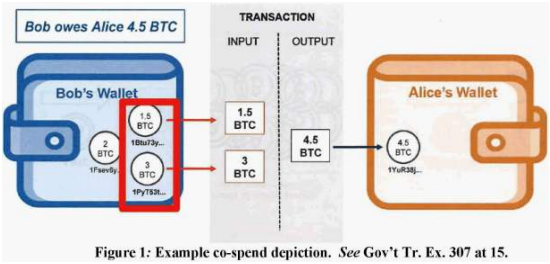

Figure 1: Example co-spend depiction. *See* **Gov't Tr. Ex. 307 at 15.**

The co-spend heuristic dates back to the creation of the Bitcoin system in late 2008 and early 2009. A white paper prepared by the inventor of the Bitcoin system recognized this weakness in the purported anonymity of the system, observing that "[s]ome linking is ... unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner." *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at

6 (2008), https://bitcoin.org/bitcoin.pdf. In a 2013 article, Professor Sarah Meiklejohn and her team of researchers from the University of California at San Diego and George Mason University, described the co-spend heuristic as based on "an inherent property of the Bitcoin protocol" and recognized that it had "already been used many times in previous work." Meiklejohn at 5. As her paper explains, the heuristic is "quite safe: the sender in the transaction must know the private signing key belonging to each public key used as an input, so it is unlikely that the collection of public keys [is] controlled by multiple entities (as these entities would need to reveal their private keys to each other)." *Id.* at 6; *see also United States v. 155 Virtual Currency Assets*, 2021 WL 1340971, at *2, 2021 U.S. Dist. LEXIS 69035, at *4 (D.D.C. Apr. 9, 2021) ("[B]ecause users often combine multiple bitcoin addresses and use them together in the same transaction (a 'cluster'), analysis of one transaction might reveal many addresses belonging to a single individual or organization.").

***5** The defense responds that "CoinJoin" services enable different individuals to contribute inputs to a single transaction, thereby defeating the assumption that when multiple addresses fund a single transaction, they are controlled by one entity. But Bisbee attests that Chainalysis has "controls in place to detect CoinJoin" and that it "can skip the CoinJoin co-spends" in its clustering. Dkt. 149-1 at 3 (Bisbee Decl.); *see also* Dkt. 229 at 243 (Aug. 23, 2023 Hrg. Tr.) (Still) (testifying that most blockchain analytics companies are able to identify transactions that occur through Wasabi, one of the most common CoinJoin implementations).

The second heuristic ("Heuristic 2") is based on observing and tracking a particular entity's on-chain behaviors and patterns. The theory underlying Heuristic 2 is that every large-scale participant in the blockchain leaves a digital "fingerprint," which can be discerned by looking at the information publicly available on the blockchain ledger and conducting test transactions with addresses known to belong to the target entity. *See* Dkt. 187 at 2 n.1. Once those behaviors have been identified, an algorithm can be used to cluster the potentially thousands of addresses that engage in transactions that match the pattern. *Id.* at 2–3 n.1 (describing how "rules are customized for each entity" in Heuristic 2 "based on close study of that entity and an understanding of the particular pattern in which the addresses within the cluster interact").

Given the risk that revealing the precise details regarding Heuristic 2 would permit cybercriminals to circumvent detection in ongoing investigations, Chainalysis provided those details to defense counsel pursuant to a protective order, *see* Dkt. 210; Dkt. 213, and the Court will, for present purposes, explain the heuristic only at a more general level, using examples. To begin, the heuristic might look to the address type employed and the behavior of the virtual wallet software used by the entity, especially as it relates to "change" addresses. By way of background, blockchain participants typically "store their private keys securely in a digital wallet, which 'can take the form of software or hardware.' " *Harmon*, 474 F. Supp. 3d at 82 (quoting Shawn Amuial *et al.*, The Blockchain: A Guide for Legal & Business Professionals § 1:9 (2016)). As noted above, the fee charged for mining (*i.e.*, verifying and transmitting a bitcoin transaction) can vary based on the speed (or priority) with which the sending entity seeks to effectuate the transaction. In addition, when the sending entity holds more bitcoin in the sending address than is necessary to complete the transaction, only some of the bitcoin in the sending address are sent to the receiving address, and the remaining amount is sent to what is referred to as the "change" address. (The Bitcoin system does not permit a user to spend only a portion of the bitcoin held in a given sending address, necessitating the creation of a "change" address to receive the unspent bitcoin.) Software wallets, moreover, "have distinctive ways of handling [1] fees and [2] change addresses," permitting Chainalysis to "investigate[ ] a service's particular transaction patterns" and to "develop clustering algorithms specific to that service." Bisbee Expert Report at 6. Through repeated observation, Chainalysis can track unique features, such as the "size of the data contained in the transaction" or the "[l]ock time" (which is "a parameter that schedules a minimal time before the blockchain accepts a transaction"). *Id.* at 7; *see also id.* at 9; Dkt. 24 at 106–07 (June 23, 2023 Hrg. Tr.) (Bisbee).

***6** Chainalysis can then use these unique characteristics to identify and to cluster addresses involving the same darknet service. In one case, for

example, a darknet marketplace employed a sliding scale for miner transaction fees such that the fee the marketplace paid varied depending on the size of a transaction—in effect, the service paid more so that the Bitcoin network would record larger transactions more quickly. *See* Andy Greenberg, *Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency* 170 (2022). By using this marker, along with many others, Chainalysis was then able to cluster together the addresses controlled by that marketplace. *Id.* Part of the reason that Heuristic 2 works is that "bigger clusters tend to be more predictable in terms of their behavior" because "the operators of these big clusters use automated scripts in order to form their transactions." George Kappos *et al., How to Peel a Million: Validating and Expanding Bitcoin Clusters*, arXiV (Cornell University) 1, 11 (2022), https://arxiv.org/abs/2205.13882 (hereinafter "Kappos"); *see* Dkt. 149-2.

Heuristic 2 also employs another technique, first discussed by Professor Meiklejohn, known as "peel chain behavior." Bisbee Expert Report at 8 (capitalization altered). As noted above, the Bitcoin system does not permit a user to expend only a portion of the bitcoin held in an address; instead, when the user wants to engage in a transaction requiring fewer than all of the bitcoin in the address, the remainder—or "change"—is sent to a change address, which remains under the control the original sender. "A peel chain is a pattern of Bitcoin transactions that occurs when a wallet receives a relatively large amount of [b]itcoin[,] which it gradually spends in multiple, sequential transactions." Scholl Expert Report at 5. "Typically, each transaction has one input and two outputs: one output constituting a payment to a separate entity and one output constituting the 'change' ... sent to a new Bitcoin address [that] is controlled by the same wallet as the input address." *Id.* This process can repeat itself through a series of transactions, creating a chain in which "[t]he 'peel' refers to the smaller, spending transaction and the 'chain' refers to the linked change addresses that continue on." Bisbee Expert Report at 8. Although, absent other information, the peel chain itself will not necessarily reveal which is the "peel," or payment, and which is the "change" address, Bisbee explains that when Chainalysis "finds the end of the chain and finds a co-spend with an address that appeared at the beginning of the chain," it can then "demonstrate[ ] that the full peel chain is controlled by the same wallet." *Id.* In other words, finding an address at the end of a chain that has co-spent with an address at the beginning of the chain makes clear which addresses are in fact change and which are in fact payment. The following diagram offers a simple example of a peel chain:

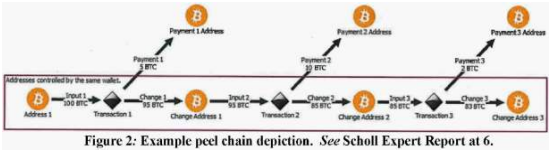

Figure 2: Example peel chain depiction. *See* **Scholl Expert Report at 6.**

The third heuristic used by Chainalysis is the so-called intelligence-based heuristic ("Heuristic 3"), which is not actually a heuristic at all. It refers, instead, to information that Chainalysis has gathered off-chain, from sources such as "data leaks, court documents, Chainalysis data partnerships, exchanges that share their addresses with Chainalysis, and manual merges due to services changing wallets." Bisbee Expert Report at 9. Unlike Heuristics 1 and 2, which analyze the blockchain, this heuristic relies on information obtained from sources unrelated to any on-chain activity or analysis. Indeed, Jonelle Still—an employee of Ciphertrace, who the defense had originally noticed as a testifying expert, *see* Dkt. 243 ("withdrawing the Ciphertrace expert report and not calling Ciphertrace expert Ms. Still as a testifying expert witness") —explained during her *Daubert* hearing that what Chainalysis calls Heuristic 3, Ciphertrace simply calls "direct attribution." Dkt. 228 at 150 (Aug. 22, 2023 Hrg. Tr.) (Still). At any rate, in the instant case, Heuristic 3 was used in a very limited capacity, only (along with Heuristics 1 and 2) to cluster addresses attributed to the darknet marketplace AlphaBay. Dkt. 232 at 107 (Sept. 7, 2023 Hrg. Tr.). The government seized AlphaBay, *see id.*, and Chainalysis reports that it "received Alphabay addresses from a data sharing agreement with the US government," Bisbee Expert Report at 16.[2]

[2] Bisbee's original report describes these three heuristics. A subsequent, more detailed explanation of the heuristics used in this case, *see generally* Dkt. 210 (discussing this additional production); Dkt. 213 (same), however, identified a fourth heuristic, *see* Dkt. 234 at 60–61 (Sept. 13, 2023 Hrg. Tr.). The government has represented that the fourth

> heuristic was not used to generate the Bitcoin Fog cluster and was otherwise so marginal to this case as to have no impact on any of Bisbee's findings as summarized in her report. *Id.* at 61–62. For that reason, the Court will discuss only the three heuristics that were addressed in Bisbee's original expert report and at the *Daubert* hearings.

***7** As used by Scholl and Bisbee in this case, Reactor employed each of the three heuristics, but in varying degrees depending on the darknet entity at issue. For the Sheep Market, for example "[o]ne hundred percent of the clustering ... was dependent on Heuristic 1," and for Evolution Market and Agora Market, almost all of the clustering (99.86% and 99.43%, respectively) was dependent on Heuristic 1. *Id.* at 25, 18, 19. For other darknet markets, Reactor used Heuristics 1 and 2 in the following percentages: Nucleus Market (55.54% Heuristic 1, 44.46% Heuristic 2), *id.* at 20; Abraxas Market (79.52% Heuristic 1, 20.48% Heuristic 2), *id.* at 22; and Pandora Market (78.49% Heuristic 1, 21.51% Heuristic 2), *id.* at 23. For AlphaBay, Reactor relied on all three heuristics. *Id.* at 16. Finally, for Bitcoin Fog, Reactor relied on Heuristic 1 (50.26%) and Heuristic 2 (49.74%) to cluster addresses. *Id.* at 13.

The question before the Court is whether Chainalysis Reactor, and Scholl and Bisbee's use of that software, passes muster under *Daubert* and Federal Rule of Evidence 702. The defense argues that "the [g]overnment's 'blockchain analysis' is junk science." Dkt. 76 at 3 (capitalization altered); *see also, e.g.*, Dkt. 45 at 8 ("We are asked to trust the [g]overnment's guesses ... through a convoluted process laden with speculative junk science ...."); Dkt. 55 at 5 ("the pervasive error, speculation, and junk science at the heart of the [g]overnment's case"); Dkt. 57 at 9 ("the Government primarily bases its case on ... junk forensics"); Dkt. 59 at 14 ("It is the Defense's position that the Government's blockchain analysis is junk science ...."). More specifically, the defense maintains that because Reactor's heuristics have not been peer reviewed and because Chainalysis does not track its rate of false positives, *see* Dkt. 149-1 at 4 (Bisbee Decl.), any testimony based on Reactor is too unreliable to satisfy the *Daubert* standard, *see, e.g.*, Dkt. 232 at 77 (Sept. 7, 2023 Hrg. Tr.) ("The problem is we have no data set, no scientific data set with which we can measure the reliability and the accuracy of this software."); *see generally id.* at 77–100. For the reasons explained below, the Court is persuaded that it is more likely than not that the evidence at issue is "the product of reliable principles and methods" and that Scholl and Bisbee's testimony will assist the jury in understanding the overwhelming mass of data found on the blockchain. The defense, of course, may question the government's evidence at trial, including the accuracy of the clusters of Bitcoin addresses generated using Reactor, and the jury will ultimately decide whether to credit the government's evidence.

II. LEGAL STANDARD

A district court has "broad discretion in determining whether to admit or exclude expert testimony." *United States ex rel. Miller v. Bill Harbert Int'l Constr., Inc.*, 608 F.3d 871, 895 (D.C. Cir. 2010) (internal citation and quotation marks omitted). Federal Rule of Evidence 702 provides that a qualified expert may testify if the "proponent demonstrates to the court that it is more likely than not that:"

> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
>
> (b) the testimony is based on sufficient facts or data;
>
> (c) the testimony is the product of reliable principles and methods; and
>
> (d) the expert's opinion reflects a reliable application of the principles and methods to the facts of the case.

In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993), the Supreme Court identified certain factors that can inform the reliability analysis under Rule 702. Those factors include: (1) whether the expert's theory or technique "can be (and has been) tested;" (2) whether it has been "subjected to peer review and publication;" (3) its "known or potential" error rate; and (4) whether it has attracted widespread acceptance within a relevant scientific community. *See id.* at 593–94, 113 S.Ct. 2786. But as the Supreme Court explained in *Kumho Tire Co. v. Carmichael*, 526 U.S.

137, 119 S.Ct. 1167, 143 L.Ed.2d 238 (1999), "the test of reliability is 'flexible,' and *Daubert*'s list of specific factors neither necessarily nor exclusively applies to all experts or in every case," *id.* at 142, 119 S.Ct. 1167. Ultimately, the trial court must assess the reliability of the expert testimony at issue based on "the particular circumstances of the particular case" and should apply, or decline to apply, the specific *Daubert* factors "depending on the nature of the issue." *Id.* at 150, 119 S.Ct. 1167 (internal quotation marks omitted).

III. ANALYSIS

***8** Against this backdrop, it is important to place the government's reliance on Chainalysis Reactor in context. This is not a case in which the government's theory that Sterlingov was the operator of Bitcoin Fog turns exclusively, or even primarily, on Scholl and Bisbee's use of the Reactor software. *See, e.g.*, Dkt. 224 at 120–21 (June 23, 2023 Hrg. Tr.) (Bisbee); Dkt. 222 at 4–5 (defense filing arguing that Reactor is only a small part of the government's case). Rather, in its effort to establish that crucial point, the government relies in substantial part on materials found in Sterlingov's possession when he was arrested, various posts on an online forum called Bitcoin Talk, internet protocol ("IP") analyses showing an individual accessing accounts directly linked to the Bitcoin Fog administrator and accounts directly linked to Sterlingov in close temporal proximity to one another, and traditional blockchain tracing that Scholl performed one Bitcoin address at a time. In the words of the defense, the testimony that will be offered based on the use of the Reactor software constitutes a "minor witness" in the case. Dkt. 222 at 5.

Nor is this a case in which the government relies on a black box, which it has declined to disclose to the defense. The defense has received reams of material explaining how the clustering was done and, at the Court's urging, received a highly confidential, supplemental production that contained additional detail about the specific methods employed as part of Heuristic 2. *See generally* Dkt. 210 (discussing this additional production); Dkt. 213 (same). The defense, moreover, has all of the underlying addresses and data and has had ample opportunity to perform its own tracing to assess the accuracy of the clustering results (or at least a representative sampling of the results) generated by the software. As discussed below, many of the results generated by Reactor have been confirmed by traditional blockchain analysis performed both before and after government witnesses used Reactor. Nothing has kept the defense from performing its own blockchain traces in an effort to refute the results generated using Reactor.

Much of the government's use of the Reactor clustering, moreover, does not involve issues requiring precise line drawing; most notably, Scholl and Bisbee have used the software to gauge the general magnitude of the transactions involving Bitcoin Fog and various darknet sites, like AlphaBay, Evolution, Agora, and Pandora. This is not to say that *Daubert* has no place in the Court's analysis of that clustering; it certainly does. But the question whether the software reliably clusters hundreds of thousands of addresses to gauge the magnitude of illicit activity is very different from the question whether it has correctly identified a single address (or handful of addresses). At least in that context, a handful of errors (if any) among hundreds of thousands of addresses is likely immaterial. *See* Dkt. 234 at 61–62 (Sept. 13, 2023 Hrg. Tr.).

In challenging the government's use of the Reactor software, the defense focuses exclusively on subsection (c) of Rule 702. *See* Fed. R. Evid. 702(c) (whether "the testimony is the product of reliable principles and methods"). The defense does not dispute that the testimony at issue "will help the trier of fact to understand the evidence or to determine a fact in issue;" that "the testimony is based on sufficient facts or data;" or that "the expert's opinion reflects a reliable application of the principles and methods" at issue. Fed. R. Evid. 702(a), (b), and (d). Indeed, when the Court inquired whether the defense wished to raise "any of the other 702 issues," the defense did not clearly raise any. Dkt. 232 at 87 (Sept. 7, 2023 Hrg. Tr.). But even if the defense had launched a broader challenge, the Court would be unpersuaded. The amount of data recorded on the blockchain is staggering, *see* Understanding 460 Million Bitcoin Addresses and Economic Activity, Chainalysis, https://www.chainalysis.com/blog/bitcoin-addresses/ (Dec. 19, 2018) (in 2018, over 460 million addresses were recorded on the blockchain), and no jury could possibly discern

whether a particular darknet site, for example, had made significant use of a bitcoin mixer without the use of a tool like Reactor. The "facts or data" that Scholl and Bisbee used, moreover, is plainly sufficient; they are derived from an immutable, public ledger, which is available for all to see. Finally, assuming that Reactor is itself reliable, there is no question that Scholl and Bisbee applied that tool in a reliable manner; they are both very experienced in the use of Reactor.

***9** The defense, instead, maintains that the government's reliance on Reactor fails each of the four *Daubert* factors, which principally concern subsection (c) of Rule 702. Those factors are: (1) "Whether a 'theory or technique ... can be (and has been) tested;' " (2) "Whether it 'has been subjected to peer review and publication;' " (3) "Whether, in respect to a particular technique, there is a high 'known or potential rate of error' and whether there are 'standards controlling the technique's operation;' " and (4) "Whether the theory or technique enjoys 'general acceptance' within a 'relevant scientific community.' " *Kumho Tire Co.*, 526 U.S. at 149–50, 119 S.Ct. 1167 (quoting *Daubert*, 509 U.S. at 592–94, 113 S.Ct. 2786) (alterations in original). As explained above, however, these factors are not cut in stone and, indeed, trial courts are required to adapt their inquiry to the unique circumstances of the case at issue. The question posed by Rule 702(c) is whether the testimony is based on "reliable principles and methods," and, in making that assessment, trial courts have substantial "latitude [both] in deciding *how* to test an expert's reliability" and in deciding "*whether or not* that expert's testimony is reliable," *Kumho Tire*, 526 U.S. at 152, 119 S.Ct. 1167 (emphases added). Here, the Court finds that Reactor easily clears the threshold for reliability, and thus admissibility, set by Rule 702(c) and *Daubert*. *See also* Feb. 22, 2024 AM Trial Tr. at 58–60 (ruling from the bench). The Court is persuaded by the ample corroborating evidence and testimony that Reactor's reliability has been established by a preponderance of the evidence in this case.

A.

The testimony that Scholl and Bisbee gave during their respective *Daubert* hearing testimony is both probative and persuasive. Scholl has worked as a cybersecurity specialist with the FBI since 2015 and is currently detailed to the Department of Justice's National Cryptocurrency Enforcement Team, serving as the lead tracing analyst for the group. Dkt. 124-1 at 1. He has used Reactor since 2016 in numerous investigations and, based on this real-world experience, he confirms that it is highly reliable. *See* Scholl Expert Report at 8. Notably, he testified as follows at his *Daubert* hearing:

> A. ... Every time we send a subpoena to an exchange to get back account information, we have the opportunity to check [whether] those Bitcoin addresses that belong to this account at this exchange were properly attributed by Chainalysis to the exchange that we subpoenaed.
>
> Q. So breaking that down a bit more, if you see funds in Chainalysis going to what Chainalysis has clustered and attributed as an exchange, you send the exchange a subpoena for records from that address. Is it your testimony that the response back from the exchange[,] verifying with records from that address that the exchange does control that address[,] ... validat[es] Chainalysis's clustering?
>
> A. Yes, ma'am, I believe it is.
>
> Q. Do you have a—is this something that you and your colleagues do frequently in your blockchain analysis type cases?
>
> A. Yes, ma'am. We do this every day.
>
> Q. Do you have a sense of the rough estimate of the volume there?
>
> A. I'd imagine a thousand times a day throughout the FBI; not me personally.

Dkt. 224 at 56 (June 23, 2023 Hrg. Tr.) (Scholl). At trial, Scholl confirmed this testimony, explaining that he could not "recall a time that [he] reviewed a subpoena where [the] Chainalysis attribution wasn't correct." Feb. 23, 2024 Trial Tr. at 16 (Scholl); *see also id.* at 17 (Scholl) ("analyz[ing] all of the subpoena returns that [he] used in [his] analysis for this case and f[inding] no false positives").

Bisbee testified at her *Daubert* hearing that, when she used Chainalysis as a specialist at the Drug Enforcement Agency ("DEA"), her

experience was consistent with Scholl's—Chainalysis clustered addresses and those clusters were routinely corroborated through legal process or through evidence recovery. Dkt. 224 at 101–102 (June 23, 2023 Hrg. Tr.) (Bisbee). While working at Chainalysis, moreover, she has verified Chainalysis clustering in a similar manner, only now through feedback she receives from Chainalysis's customers, including large exchanges. *Id.* at 116–18 (Bisbee). She testified as follows:

> Q. Could you speak, generally, without divulging any sort of sensitive details on a particular case, about instances where Chainalysis Reactor is used and has been found to be reliable[?]
>
> A. So in all of the investigations that my team supports, we provide investigative reports to our public sector customers. They're then able to leverage that to further their investigations, and we have never, in the last two and a half years I've been with Chainalysis, ever received anything back that says that it was not correct or that it was incorrectly attributed for the information we provided.

***10** *Id.* at 134 (Bisbee).[3] Indeed, Bisbee explained that the typical feedback she receives is that Chainalysis's clustering and attribution is, if anything, *underinclusive*—because the company takes a "conservative approach" to clustering. *Id.* at 118 (Bisbee). She testified that in her work at the DEA, and now at Chainalysis, spanning hundreds of investigations, with the clustering of thousands upon thousands of addresses, she is not aware of a *single false positive* encountered by her or anyone working with her. *Id.* at 138–39 (Bisbee).

3 Although Bisbee testified earlier during the *Daubert* hearing that Chainalysis receives feedback from clients when they get "false hits," she clarified a few moments later that the feedback Chainalysis typically receives is that Reactor's clustering was underinclusive. *Id.* at 116–18. And, as noted above, she also testified that she had never received any feedback indicating that Reactor's clustering incorrectly had attributed addresses.

In a sealed supplemental filing, the government offered additional corroboration of Reactor's reliability. As that filing explains, a confidential cooperating defendant reviewed a large number of addresses clustered by Chainalysis and confirmed that 99.9146% had been correctly clustered and attributed. *See* Dkt. 193 at 8 & n.1; *cf. In the Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d 1, 20 (D.D.C. 2022) ("[I]n an unrelated case, [Redacted] clustering software directed the government to over 50 customers of a darknet child pornography site. In each one of the 50 subsequent law enforcement actions, the software's data was corroborated by statements and search warrant returns from the targets' devices." (alteration in original)).

Reactor's reliability is further corroborated by the investigation that was conducted in this case. First, as Scholl discusses in his report, the FBI and the Internal Revenue Service, Criminal Investigation ("IRS-CI") conducted sting transactions directly with Bitcoin Fog by accessing Bitcoin Fog's Tor hidden services address on the darknet and making deposits and withdrawals there. Scholl Expert Report at 8–10. Those undercover transactions led Scholl to attribute, by hand, five Bitcoin addresses to Bitcoin Fog. *Id.* at 11. Chainalysis Reactor correctly had attributed four of the five addresses to the Bitcoin Fog cluster. *Id.* It did not include the fifth address in the Bitcoin Fog cluster because it is deliberately conservative and thus underinclusive; Reactor did, however, cluster an address closely associated with the fifth address as Bitcoin Fog—the address which had sent funds to that fifth address. *Id.* At least as used in this case, the fact that Reactor is conservative—that is, if in doubt, do not include the address—is hardly reason to discount its reliability. To be sure, four addresses is a small subset of the Bitcoin Fog cluster, but Reactor's performance on that subset speaks to its reliability given the random nature with which its accuracy was tested. Reactor correctly attributed four addresses to the Bitcoin Fog cluster, as confirmed by Scholl's hand tracing, out of hundreds of millions Bitcoin addresses. The hand-tracing that Scholl conducted following the FBI and IRS-CI sting transactions, thus, corroborates the clustering by Chainalysis.

In addition, although Reactor was primarily used to link Bitcoin Fog to darknet marketplaces, the government identified 43 transactions which sent funds from 144 unique addresses within the Bitcoin Fog cluster to Sterlingov's accounts. *Id.* at 11; *see* Dkt.

232 at 49 (Sept. 7, 2023 Hrg. Tr.). Reactor clustered the 144 addresses as Bitcoin Fog, and the blockchain analysis tool, TRM Labs, corroborated the attribution for all 144 of those addresses. Scholl Expert Report at 11.

***11** But it is not just the government's evidence that supports Reactor's reliability: The defense itself has provided evidence of Reactor's reliability through (1) the pretrial testimony of Sterlingov himself, and (2) the pretrial testimony of its then-testifying witness, Jonelle Still of Ciphertrace. To start, Sterlingov testified under oath at a pretrial proceeding that the bitcoin in his Kraken account arrived there after being mixed in Bitcoin Fog, thereby conceding "the very thing that the government was trying to prove through its blockchain analysis." Dkt. 116 at 16 (Memorandum Opinion). Scholl independently confirmed this, in part through the use of Reactor's clustering. *See* Scholl Expert Report at 8, 21–22, 25–26.

As for Still, she observed in her expert report that her employer, Ciphertrace, "also uses Heuristic 1 Multi-input Clustering as the *primary heuristic* for non-direct attribution." Dkt. 159-1 at 28 (Still Expert Report) (emphasis added). Before the Court, Still testified about the contents of an affidavit she submitted in another case, in which she affirmed that the "co-spend technique is *highly reliable and the most-used metric* in commercial blockchain analysis tools." Dkt. 228 at 163 (Aug. 22, 2023 Hrg. Tr.) (Still) (emphasis added).[4] And, with respect to Heuristic 3, Still testified that Ciphertrace uses its own version of that heuristic but refers to it as "direct attribution," instead of as a heuristic. *Id.* at 150 (Still). Finally, with respect to Heuristic 2, although Still originally opined that the heuristic is "error-prone," Dkt. 159-1 at 8 (Still Expert Report), defense counsel subsequently informed the Court that Ciphertrace is currently developing its own version of Heuristic 2, casting substantial doubt on Still's original view, *see generally* Dkt. 210 (Memorandum Opinion).

4 Still was reading, at the government's request, from a sworn affidavit she submitted in another case. Dkt. 228 at 158–61 (Aug. 22, 2023 Hrg. Tr.) (Still). Although Still pointed out that the underlying case concerned a different type of cryptocurrency, Ether, on the Ethereum network, *id.* at 161 (Still), the language of the affidavit as read into the record by Still plainly discusses clustering for "cryptocurrency" writ large, not specifically Ether.

Beyond using similar methods, Chainalysis and Ciphertrace also arrived at substantially similar results in important respects. For example, Chainalysis attributed over 900,000 addresses to the Bitcoin Fog cluster, and Still testified that Ciphertrace agreed with respect to almost 400,000 of those addresses.[5] Dkt. 228 at 189 (Aug. 22, 2023 Hrg. Tr.) (Still). With respect to the 500,000-address delta, however, Still was unable to identify any address or set of addresses that Ciphertrace had determined was *not* Bitcoin Fog and that Chainalysis had mistakenly included in the Bitcoin Fog cluster. *Id.* at 177–79 (Still). In other words, Ciphertrace was unable to identify a single false positive and actually confirmed almost 400,000 of the addresses at issue; the fact that Ciphertrace was even more conservative (or arguably less adroit) in its analysis does not cast doubt on the reliability of Reactor's results. Finally, it is also noteworthy that Ciphertrace and Chainalysis's darknet cluster attributions largely align with respect to several darknet marketplaces, including Agora (3.5% difference), Sheep (0% difference), Silk Road 2.0 (0% difference), and WelcomeToVideo (1% difference). Dkt. 159-1 at 35 (Still Expert Report).[6]

5 Moreover, Still's testimony on cross examination suggests that the Chainalysis and Ciphertrace clusters for Bitcoin Fog are even more similar than Still's report initially indicated. The government elicited on cross examination that Chainalysis had clustered 575,213 addresses into the Fog cluster *all based on Heuristic 1*, but Still erroneously believed that figure was just 398,011 because she misread an appendix provided by Chainalysis that contained a guide for how to parse its data. *Id.* at 185 (Still). Still's analysis was off by approximately 200,000 addresses, leading the Court to conclude that the 500,000-address delta between the Chainalysis and Ciphertrace Bitcoin Fog clusters is, in all likelihood, considerably smaller.

6 As Still clarified in her testimony, the percentage figures in her report are not error rates; rather she used them to quantify how many *more* addresses Chainalysis clustered as compared to

Ciphertrace. Dkt. 228 at 123–24 (Aug. 22, 2023 Hrg. Tr.) (Still).

***12** For all of these reasons, the Court concludes by a preponderance of the evidence that—at least as used in this case and as confirmed by the other evidence before the Court, including Sterlingov's own pretrial testimony—Chainalysis Reactor is reliable.[7]

[7] Earlier in the life of this case, there was dispute over the use of the word "deterministic" to describe Reactor; the government and Chainalysis, however, have made clear that Reactor is deterministic in the sense that when Reactor is run on a fixed data set, its algorithm will produce the same results (clusters) every time. *See* Dkt. 149-1 at 3 (Bisbee Decl.). In other words, Reactor performs consistently.
In response to the defense's concerns about Reactor performing consistently, the Court made clear that it believed the defense was "entitled to run the analysis and to make sure you get the same result [as the government] using Reactor." Dkt. 228 at 31 (Aug. 22, 2023 Hrg. Tr.). To that end, the Court invited the defense to apply to the Court for funding to seek a Reactor license or, if more cost-effective, for funding to retain an expert with his or her own Reactor license. *Id.* at 31–33. At the time, Sterlingov was still proceeding *in forma pauperis* and receiving funding pursuant to the Criminal Justice Act ("CJA"). *See* Dkt. 118. The Court directed the defense to "follow [its] instructions promptly and [ ] find out how much the license is," noting that if it "need[ed] to authorize a payment ... [it would] do so." *Id.* at 33; Dkt. 229 at 80 (Aug. 23, 2023 Hrg. Tr.) ("As I've said, if someone just asks me to authorize funding for a license ... I'm prepared to do that."). The defense never followed through and applied for CJA funding to obtain a Reactor license, and subsequently, Sterlingov withdrew his request to proceed *in forma pauperis*. Dkt. 234 at 83 (Sept. 13, 2023 Hrg. Tr.) ("I've already told Mr. Ekeland multiple times that he can obtain a license or find somebody with a license and run the software. And although he withdrew from CJA today, before that I already told him that I would approve a CJA voucher which he never filed with respect to seeking a license for the Reactor software."); *see id.* at 107–09; *see also* Min. Entry (Sept. 15, 2023).

B.

The Court's analysis could end there. But, because the defense argues that "Chainalysis Reactor doesn't meet any of the *Daubert* factors, not one," Dkt. 232 at 91 (Sept. 7, 2023 Hrg. Tr.), the Court will briefly explain why that is not the case. At the outset, the Court observes, once again, that the *Daubert* factors "do *not* constitute a definitive checklist or test." *Kumho Tire*, 526 U.S. at 150, 119 S.Ct. 1167 (emphasis in original). As the D.C. Circuit recently noted, "the *Daubert* factors 'may or may not be pertinent in assessing reliability' in specific circumstances." *United States v. Morgan*, 45 F.4th 192, 203 (D.C. Cir. 2022) (internal citation omitted). Instead, the "reasonable measures of reliability in a particular case is a matter that the law grants the trial judge broad latitude to determine," *Kumho*, 526 U.S. at 152–53, 119 S.Ct. 1167; *see also United States v. Straker*, 800 F.3d 570, 631 (D.C. Cir. 2015) (holding that the district court did not abuse its discretion in denying motion to strike and subsequent motion for a new trial based on admission of fingerprint expert who did not present testimony of an error rate because the factors "listed in *Daubert* do not constitute a definitive checklist or test" and because the district court properly took the reliability of the expert's fingerprint methodology for granted).

***13** Starting with the first *Daubert* factor—"whether the theory or technique can be and has been tested," *Ambrosini v. Labarraque*, 101 F.3d 129, 134 (D.C. Cir. 1996)—the Court finds that Reactor's clustering can be and has been tested. Clustering, whether conducted by Chainalysis or any other blockchain analytics company, can be replicated by competitor software products and, on a smaller scale, by hand, because the underlying data is publicly available on the blockchain. In this case, for example, Scholl corroborated Reactor's clustering through manual tracing and through TRM Labs' software. *See* Scholl Expert Report at 9–11. Similarly, Still was able to run the same blockchain data through Ciphertrace's competing clustering software and to create a Bitcoin Fog cluster that differed in size from, but also shared meaningful overlap with, Chainalysis's Bitcoin Fog cluster. *See* Dkt. 157 at 2; Dkt. 159-1 at 8 (Still Expert Report); Dkt. 228 at 189 (Aug. 22, 2023 Hrg. Tr.) (Still). That Still reached an overlapping but less

expansive result does not negate the fact that she was able to test Reactor's clustering.

Second, with respect to peer review and publication, Chainalysis Reactor has not itself been subject to peer review, but the co-spend heuristic has received widespread academic approval. As discussed above, "Heuristic 1" not only has it its origins in the white paper inventing bitcoin, but it has also been widely discussed and relied upon in academia. *See* Meiklejohn at 6 (recognizing that co-spend "has already been used many times in previous work"). The notion of "peer review" in the context of Heuristic 2, moreover, is an odd fit: As explained, Heuristic 2 varies from case-to-case and entity-to-entity because Chainalysis identifies distinct digital behaviors—or tells—for each darknet market or service for which it is seeking to cluster addresses and then incorporates those features in an algorithm. Bisbee Expert Report at 6. Thus, the fact that the Heuristic 2 algorithms developed for the darknet services at issue in this case have not been the subject of peer review is neither surprising nor dispositive. As *Daubert* itself made clear "[t]echnical fields need not be held to the standard of peer review applicable to traditional sciences, which are often considered in scholarly journals." *United States v. Frabizio*, 445 F. Supp. 2d 152, 165 (D. Mass. 2006) (citing *Daubert*, 509 U.S. at 593–94, 113 S.Ct. 2786); *Daubert*, 509 U.S. at 593, 113 S.Ct. 2786 ("Publication (which is but one element of peer review) is not a sine qua non of admissibility; it does not necessarily correlate with reliability."). And, as the D.C. Circuit recently observed, a court may "understandably decline[ ] to automatically exclude evidence because it is too new, or of too limited outside interest, to generate extensive independent research or peer-reviewed publications." *Morgan*, 45 F.4th at 203 (quotation marks omitted).

The concept of "peer review" is also inapt when it comes to Heuristic 3, which consists of data and information obtained off-chain from, among other things, Chainalysis's clients and partners (which include global cryptocurrency exchanges), government subpoenas, and data leaks. Bisbee Expert Report at 9. To be sure, Professor Meiklejohn and her team have observed that when they engaged in similar practices without the subpoena power (cataloguing addresses that they found on various forum and blog posts), they "regarded this [ ] kind of tagging as less reliable than our own observed data." Meiklejohn at 4. But a jury is well equipped to decide, through cross examination, whether addresses clustered based on blog posts and data leaks are less reliably de-anonymized than those addresses that are identified through the subpoena power or through exchanges voluntarily sharing user information with Chainalysis. In the decade since Meiklejohn made that observation in 2013, moreover, academic research focused on cryptocurrency, the blockchain, and blockchain analytics has only grown alongside the industry.[8] Finally, the Court notes that, in this case, the government relies on Heuristic 3 only as applied to the AlphaBay cluster and, even there, it was used in combination with Heuristics 1 and 2. Bisbee Expert Report at 16.

8 *See, e.g.*, Kappos at 2 (summarizing noteworthy scholarship on clustering and collecting citations). Chainalysis has shared its data with researchers, *see, e.g., id.*, and Chainalysis's own staff researchers have submitted scholarly articles, both on their own and as part of larger University-led research teams, *see, e.g.*, Daniel Goldsmith *et al., Analyzing Hack Subnetworks in the Bitcoin Transaction Graph*, arXiV (Cornell University) (2019) https://arxiv.org/abs/1910.13415; Alberto Bracci *et al., Macroscopic Properties of Buyer-Seller Networks in Online Marketplaces*, arXiV (Cornell University) (2021) https://arxiv.org/abs/2112.09065; *see also* Dkt. 73 at 14 & n.4.

***14** With respect to the third *Daubert* factor —"the method's known or potential rate of error," *Ambrosini*, 101 F.3d at 134—Bisbee explained that Chainalysis "has not gathered and recorded in a central location false positives/false negatives because [it] is design[ed] to be more conservative in the clustering of addresses." Dkt. 149-1 at 4 (Bisbee Decl.).[9] The lack of a compiled "error rate" of this sort, however, does not alter the Court's finding that Reactor is reliable. As detailed above, Scholl offered persuasive testimony concerning the lack of false positives in his extensive experience using Reactor and as confirmed by the tracing he performed in this case. Dkt. 224 at 56 (June 23, 2023 Hrg. Tr.) (Scholl); Feb. 23, 2024 Trial Tr. at 16 (Scholl). Likewise, Reactor's clustering was confirmed by clustering conducted using software from TRM

Labs. Scholl Expert Report at 11. Even the clustering by Ciphertrace and testified to by Still confirmed much of the work done by Reactor's Heuristic 1. Dkt. 228 at 189 (Aug. 22, 2023 Hrg. Tr.) (Still). Nothing more is required.[10]

9 The error rates identified in the Kappos paper pertain to different heuristics developed by prior researchers between the years of 2013 and 2018, not to Reactor's heuristics. *See* Kappos at 12, 15–16; Dkt. 229 at 257–68 (Aug. 23, 2023 Hrg. Tr.) (Still) (discussing the error rates in the Kappos paper).

10 Like the governing caselaw, the Committee Notes to the recent amendment to Rule 702 recognize that the known or potential rate of error is not always available. *See* Fed. R. Evid. 702 advisory committee's note to 2023 amendment ("In deciding whether to admit forensic expert testimony, the judge should (*where possible*) receive an estimate of the known or potential rate of error of the methodology employed ...." (emphasis added)).

Finally, with respect to the fourth *Daubert* factor —"whether the theory or technique finds general acceptance in the relevant scientific community," *Ambrosini*, 101 F.3d at 134—the defense offers no response to the evidence that blockchain tracing, like that at issue here, is widely relied upon by both the law enforcement and business communities, *see* Dkt. 232 at 57 (Sept. 7, 2023 Hrg. Tr.) ("[Blockchain analysis] has been used extensively by law enforcement in the United States, by law enforcement all around the world, by private sector, by financial institutions, by consulting firms, by incident response firms, by regulators ...."). Chainalysis "in particular is viewed as an industry standard tool and has customers from the Department of the Treasury, the Department of Justice, the Department of Homeland Security, the Department of State, and the Consumer Financial Protection Bureau." Dkt. 73 at 19 (citing Recipient Profile: Chainalysis Inc., USASpending.gov, https://www.usaspending.gov/recipient/93c1b742-3801-7f06-775d-da2c3fff3fd6-C/latest (last visited Feb. 28, 2024)).

With respect to the private sector, major virtual currency exchanges and other financial institutions use blockchain analysis software tools as part of their anti-money laundering programs in order to comply with their regulatory obligations and monitor transactions for suspicious activity. *See* Dkt. 73 at 20–21. As Bisbee testified, large exchanges use a Chainalysis software product called KYT, named for "Know Your Transaction," for compliance purposes. Dkt. 224 at 115–16 (June 23, 2023 Hrg. Tr.) (Bisbee). KYT utilizes the same underlying data as Reactor, and, crucially, exchanges and compliance firms "rely on [Chainalysis' accuracy] in order to have credibility within the ecosystem." *Id.* at 116. This is the sort of widespread industry acceptance that the D.C. Circuit credited in *United States v. Morgan*, 45 F.4th 192 (D.C. Cir. 2022). There, in evaluating the district court's finding that the expert's testimony was "the product of reliable principles and methods," the D.C. Circuit relied in part on the fact that "drive testing technology has been relied upon, tested and reviewed for decades in the multibillion dollar wireless communications industry." 45 F.4th at 202 (citation omitted).

***15** For all of these reasons and based on the extensive testimony and expert reports in this case, the Court is persuaded that blockchain analytics in general, and Reactor in particular, is not junk science. Some of the defense's arguments might (or might not) offer fruitful ground for cross examination before the jury. The Court's role, however, is to act only as a gatekeeper, and, applying a preponderance of the evidence standard, to ensure that the testimony offered for the jury's consideration is "the product of reliable principles and methods," Fed. R. Evid. 702(c). As the Supreme Court has explained, it is not exclusion, but instead "[v]igorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof" that "are the traditional and appropriate means of attacking [arguably] shaky but admissible evidence." *Daubert*, 509 U.S. at 596, 113 S.Ct. 2786. Here, the government's blockchain tracing evidence readily clears the hurdle necessary to reach the jury.

CONCLUSION

As previously explained on the record and further explained above, the Court finds that the government has demonstrated by a preponderance of the evidence that the blockchain analysis generated by Chainalysis

Reactor is the product of reliable principles and methods, and the Court, accordingly, **DENIES** defendant's requests to exclude the testimony and evidence based on that analysis, *see* Dkt. 59; Dkt. 72; Dkt. 251.

SO ORDERED.

All Citations

--- F.Supp.3d ----, 2024 WL 860983

End of Document