IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

THE UNITED STATES OF AMERICA

v. No. 1:21-cr-41-JL-01

ARIA DIMEZZO

MOTION IN LIMINE:
DAUBERT CHALLENGE TO FORENSIC BLOCKCHAIN ANALYSIS

The accused, Aria DiMezzo, through counsel, respectfully requests that the court bar the Government from offering at trial expert and non-expert testimony regarding forensic blockchain analysis. The government cannot establish the admissibility of such evidence under Rules of Evidence 403 or 702, or under *Daubert v. Merrell Dow Pharm., Inc*., 509 U.S. 579, 113 S. Ct. 2786 (1993). The defense has not found any published case holding that forensic blockchain analysis is reliable under the *Daubert* standard, and there is good reason to believe that it is not. The court should bar the use of such evidence at trial.

The Charges and the Government's Proposed Testimony.

Ms. DiMezzo is charged in nine counts of a 33-count superseding indictment. The Government claims that DiMezzo and co-defendant Ian Freeman operated a business which exchanged virtual currency, such as Bitcoin, for U.S. Dollars. The Government claims that DiMezzo and Freeman unlawfully failed to register the business. The Government further claims that DiMezzo and Freeman committed crimes of fraud, or enabled others to commit crimes of fraud, through their activities. On the basis of those allegations, Ms. DiMezzo faces four counts of wire fraud and three counts of money laundering.

The Government has provided discovery which includes financial transactions which it says relate to the alleged illegal conduct. The financial transactions allegedly include transactions involving virtual currency, such as Bitcoin. Those transactions depend on the blockchain.

As described by a Government agent in this case:

> All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," stored on the peer-to-peer network on which the Bitcoin system operates. The Blockchain serves to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and therefore, cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system.
>
> Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

Aff. of Special Agent Kathryn Thibault, Aff. in Supp. of Search Warrants for Elec. Devices Located at 659 Marlboro Street, Keene, New Hampshire, ¶¶ 16, 17.

The Government has given notice that it is going to offer blockchain analysis evidence through both expert and non-expert witnesses. *See* Letter from Counsel for the Government to Defense Counsel, March 21, 2022. The Government proposes Erin Montgomery "as an expert witness on virtual currency and blockchain analysis." She "is expected to provide testimony explaining cryptocurrencies like Bitcoin, including how Bitcoin transactions are conducted, and how transactions can be traced on the blockchain." Her "testimony will include a discussion of the properties of cryptocurrency including those making it pseudonymous." The Government specifically says she is "expected to testify regarding clustering, a blockchain analysis technique that identifies linked addresses held by an individual or organization." Regarding the investigation in this case, the Government states that Montgomery "performed blockchain analysis in support of this investigation," that she "reviewed the blockchain—a public ledger of bitcoin transactions," and that she "followed those funds to addresses that were under the defendants' control."

In addition to the expert testimony from Montgomery, the Government says it will call non-expert witnesses who "will also provide testimony regarding virtual currency, exchanges, and blockchain analysis." The Government claims these are "fact witnesses" who will testify to "their personal knowledge and conduct of the investigation, not as expert testimony as defined in Fed. R. Evid. 702."

Forensic Blockchain Analysis.

The Bitcoin blockchain, the ledger of every transaction that ever occurred in the history of Bitcoin, is publicly available. It is currently over 400 GB in size. "Blockchain Size," *Blockchain.com*, July 27, 2022, https://www.blockchain.com/charts/blocks-size. There have been more than 750 million transactions since its inception. "Total Number of Transactions," *Blockchain.com*, July 27, 2022, https://www.blockchain.com/charts/n-transactions-total. In theory, "anyone can see any Bitcoin transaction," however, "[a]ttempted manually, such tracing is cumbersome and time consuming." C. Alden Pelker et al, *Using Blockchain Analysis from Investigation to Trial*, 69 Dep't Just. J. Fed. L. and Prac. 59, 62 (May 2021), available at https://www.justice.gov/usao/page/file/1403671/download.

The most common blockchain analysis techniques use what is called "cluster analysis" to attempt to de-anonymize Bitcoin transactions. They do so by relying on certain heuristics and assumptions. In common input or co-spend analysis ("the most-used metric in commercial blockchain analysis tools"), the blockchain analysis links addresses with the assumption that "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." *Id*. Another type of cluster analysis looks to the "address that receives any remainders of transferred funds from a transaction" with the assumption that the ultimate output address and all the original inputs "may be controlled by the same user." *Id*. These two heuristics – (1) "if two addresses have been used as input to the same transaction, they are controlled by the same user" and (2) "the change address in a transaction is controlled by the sender" – are foundational elements of forensic blockchain analysis. *See* Sarah Meiklejohn, *The Limits of Anonymity in Bitcoin*, *in Routledge Handbook of Criminal Science* (Richard Wortley et al, eds., 2018) at 285. (For a short explanation of Bitcoin heuristics, see "Introduction to Bitcoin Heuristics," *CryptoQuant*, July 30, 2019, https://medium.com/cryptoquant/introduction-to-bitcoin-heuristics-487c298fb95b.)

Blockchain analysis is only as reliable as its underlying assumptions. In theory, at least according to federal prosecutors, "clustering can be done manually" but "doing so would be cumbersome and limited; instead, law enforcement uses commercially available blockchain analysis tools to streamline the process." Pelker et al., *supra* at 62-3.

Although it is not entirely clear, it appears that in this case the Government's agent and designated expert witness may have used commercially available blockchain analysis tools. So, for example, in a June 18, 2019 FBI memo summarizing a May 29, 2019 case coordination meeting, Staff Operations Specialist Alexandra Comolli and Intelligence Analyst Erin Montgomery "provided a presentation on blockchain analysis." Alexandra Comolli & Erin Montgomery, *To Document Participation in Case Coordination Meeting* (June 18, 2019) at 2. A number of FBI memorandums in the discovery also make reference to Bitcoin blockchain analysis. *See, e.g.*, Alexandra Comolli & Erin Montgomery, *272B-BS-2234931 Serial 243* (Feb. 20, 2020); Alexandra Comolli & Erin Montgomery, *272B-BS-2234931 Serial 286* (Sept. 15, 2020); Alexandra Comolli & Erin Montgomery, *272B-BS-2234931 Serial 290* (Sept. 21, 2020); Erin Montgomery & Alexandra Comolli, *272B-BS-2234931 Serial 303* (March 8, 2021); Erin Montgomery & Alexandra Comolli, *272B-BS-2234931 Serial 304* (March 8, 2021).

The *Daubert* Standard.

"The touchstone for the admission of expert testimony in federal court is Federal Rule of Evidence 702." *Crowe v. Marchand*, 506 F.3d 13, 17 (1st Cir. 2007). Under Rule 702:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
>
> > (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 has reliably applied the principles and methods to the facts of the case.

Fed. R. Evid. 702. As explained by this court, "before the factfinder in a case can consider expert testimony over the adverse party's objection, the trial judge, serving as 'gatekeeper,' must determine whether the testimony satisfies the relevant foundational requirements." *Adams v. J. Meyers Builders, Inc.*, 671 F. Supp. 2d 262, 272 (D.N.H. 2009) (quoting *Daubert*, 509 U.S. at 597). According to the First Circuit, "this rule requires district courts to act as gatekeepers, ensuring that an expert's proffered testimony 'both rests on a reliable foundation and is relevant to the task at hand.'" *Samaan v. St. Joseph Hosp.*, 670 F.3d 21, 31 (1st Cir. 2012) (quoting *Daubert*, 509 U.S. at 597).

The reliable foundation and relevance inquiries "are separate and distinct." *Samaan*, 670 F.3d at 31. "The reliable foundation requirement necessitates an inquiry into the methodology and the basis for an expert's opinion" where the district court considers "a number of factors, including but not limited to 'the verifiability of the expert's theory or technique, the error rate inherent therein, whether the theory or technique has been published and/or subjected to peer review, and its level of acceptance within the scientific community,'" wherein "the expert's methodology is commonly 'the central focus of a *Daubert* inquiry.'" *Id.* at 31-32 (quoting *Ruiz-Troche v. Pepsi Cola of P.R. Bottling Co.*, 161 F.3d 77, 81 (1st Cir. 1998)). *See also Daubert*, 509 U.S. at 593-94 ("a preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue"). But note:

> These factors, however, are not definitive or exhaustive, and the trial judge enjoys broad latitude to use other factors to evaluate reliability. *United States v. Mooney*, 315 F.3d 54, 61 (1st Cir. 2002) (citing *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 153, 119 S. Ct. 1167 (1999)). The trial judge may even determine which of the *Daubert* factors to apply depending on the nature of the issue, the expert's

> particular expertise, and the subject of her testimony. *Kumho Tire*, 526 U.S. at 150.

United States v. Mahone, 328 F. Supp. 2d 77, 88 (D. Me. 2004).

The party seeking to introduce the expert testimony bears the burden of proving its admissibility. *Milward v. Rust-Oleum Corp.*, 820 F.3d 469, 473 (1st Cir. 2016). The Supreme Court said in *Daubert*, "[t]he inquiry envisioned by Rule 702 is, we emphasize, a flexible one." *Daubert*, 509 U.S. at 594; *see also* *United States v. Martinez-Armestica*, 846 F.3d 436, 443 (1st Cir. 2017). But in criminal proceedings, as the First Circuit said in *United States v. Shay*, 57 F.3d 126 (1st Cir. 1995), "[e]ven if expert testimony is admissible pursuant to Rule 702, it may be disallowed pursuant to Fed. R. Evid. 403 if its prejudicial, misleading, wasteful, confusing, or cumulative nature substantially outweighs its probative value." *Shay*, 57 F.3d at 134.

Procedurally, the First Circuit has said, "there is no particular procedure that the trial court is required to follow in executing its gatekeeping function under *Daubert*." *United States v. Diaz*, 300 F.3d 66, 73 (1st Cir. 2002). *See also* *Smith v. Dorchester Real Estate, Inc.*, 732 F.3d 51, 64 (1st Cir. 2013). In *Kumho Tire Co. v. Carmichael*, the Supreme Court explained how

> The trial court must have the same kind of latitude in deciding *how* to test an expert's reliability, and to decide whether or when special briefing or other proceedings are needed to investigate reliability, as it enjoys when it decides *whether* that expert's relevant testimony is reliable.…Otherwise, the trial judge would lack the discretionary authority needed both to avoid unnecessary "reliability" proceedings in ordinary cases where the reliability of an expert's methods is properly taken for granted, and to require appropriate proceedings in the less usual or more complex cases where cause for questioning the expert's reliability arises.

Id. at 152 (italics in original).

Cases and Articles Addressing the Reliability of Blockchain Analysis.

The defense challenges the Government's purported blockchain analysis because it does not meet the standards required by *Daubert*. Blockchain analysis has been addressed by courts in the context of probable cause determinations for warrants, but the defense has found no published cases in which blockchain analysis was admitted at trial over a *Daubert* objection. The defense believes this is because blockchain analysis is used primarily as an investigative technique which may lead to the discovery of more conventional evidence. In any event, in the absence of authority from other courts, the Government cannot establish admissibility at DiMezzo's trial unless it convinces this court that blockchain analysis is reliable under the *Daubert* standard. It cannot carry that burden.

The defense has found one published analysis of the *Daubert* issue, though not from a court. In 2015, the prominent scholar of evidence, Edward Imwinkelried, the University of California Davis Professor of Law Emeritus, published a joint research paper with a student in *Criminal Law Bulletin.* Jason Luu and Edward Imwinkelried, *The Challenge of Bitcoin Pseudo-Anonymity To Computer Forensics*, 52 Crim. L. Bull. 191 (2016). Lacking any "case law precedent providing evidentiary guidance about the admissibility and weight of these techniques," the pair undertook a *Kelly*/*Frye* and *Daubert* analysis. *Id*. at 16. To the first standard, they concluded, "[b]oth traffic and transaction graph analyses would most likely fail the general acceptance test" and there is "currently no evidence of extensive support for either traffic analysis or transaction graph analysis." *Id*. at 17. The authors then reviewed blockchain analysis techniques under a six-factor *Daubert* analysis. *Id*. at 18 (citing *Daubert*, 509 U.S. at 593–94). The pair found "that neither traffic analysis nor transaction graph analyses passes muster under *Daubert*" and "[o]n balance, a review of the application of the *Daubert* factors to these two techniques leads to the conclusion that in the current state of the art, trial judges should bar testimony based on these techniques." *Id*. at 19.

Prosecutors at the Department of Justice are conscious of the role of blockchain analysis in criminal prosecutions. One year ago, three DOJ attorneys published a paper surveying the use of blockchain analysis in investigations and trials. Pelker et al, *supra*. They make no reference to Imwinkelried. *Daubert* appears only briefly at the end of their paper when they note that if prosecutors seek to use expert testimony related to blockchain (specifically clustering) analysis, prosecutors "should be prepared for a potential *Daubert* hearing" and "should develop a plan to appropriately address any trade secret or law enforcement privilege issue in advance of the *Daubert* hearing." *Id*. at 98. Beyond that, they do not address the *Daubert* issues.

Nonetheless, other portions of the article hint at how blockchain forensics would fail *Daubert*'s test. The authors note how "blockchain analysis software largely serves an aggregation function" and "much of the functionality provided by blockchain analysis software lies in its ability to pull massive amounts of transactional data from the blockchain and provide user-friendly tools to explore it" and yet, the "software does not *only* aggregate blockchain data; it also applies heuristics and other analytical tools to cluster addresses into related groups." *Id*. at 69-70 (emphasis in original). Thus, when they say "[i]n theory, most analysis of blockchain transactions could be done by hand" they really mean that portions of the analysis could theoretically be done by hand—if a human were capable of manually tracking millions of transactions—but *also* that other portions rely on "heuristics" and "other analytical tools" that are unexplained and undefined. *Id*.

The authors reveal another reason why blockchain forensics stay out of the courtroom. As they explain it:

> [P]rosecutors 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.

Id. at 97.

Commercial and efficiency concerns dominate. As another group of U.S. attorneys warned in an article about cryptocurrency attribution, "[a]nticipate that proprietary algorithms or other trade secrets may also be used in commercial tools," "[t]rade secrets may need to be protected from public disclosure," and "[i]f any blockchain analysis relies upon a commercial tool, there may be limitations to the licensing of that tool to the federal government agency." Michele Korver et al, *Attribution in Cryptocurrency Cases*, 67 Dep't Just. J. Fed. L. and Prac. 233, 248 (Feb. 2019), available at https://www.justice.gov/usao/page/file/1135861/download.

A case which is not on point here but which is sometimes cited regarding forensic blockchain analysis is the Fifth Circuit's decision in *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020). In that case, the defendant moved to suppress evidence obtained from a warrant that used blockchain analysis to track Bitcoins from a child pornography website to a cryptocurrency exchange (Coinbase) that was in turn linked to the defendant. The district court denied his motion, Gratkowski entered a conditional guilty plea and appealed to the Fifth Circuit. *Id*. at 309-10. The court affirmed the district court, announcing that Gratkowski lacked a reasonable expectation of privacy in his bitcoin transactions or his Coinbase records. *Id*. 310-13. The court did not analyze the issue of blockchain analysis's reliability. The court simply said, "due to [the public nature of the blockchain], it is possible to determine the identities of Bitcoin address owners by analyzing the blockchain." *Id.* at 312. The court then cited to the original paper proposing Bitcoin by Satoshi Nakamoto. *Id*. at 312, fn.6. The court did not engage in any other analysis.

Gratkowski's legacy is seen in *United States v. Dove*, No. 8:19-cr-33-T-36CPT, 2020 U.S. Dist. LEXIS 251313 (M.D. Fla. Sep. 4, 2020). *Dove* involved a *Franks* hearing before a magistrate judge in Florida, where the defendant, charged with multiple child pornography offenses, alleged the search warrant used in his investigation involved omitted and false statements. *Id.* at *3. In rejecting Dove's allegations, the magistrate found information in the law enforcement affidavit sufficient to establish probable cause. *Id.* at *34-5. In particular, the judge credited the affidavit's assertions that:

> Although the blockchain contains very little information about the BTC senders and recipients, blockchain analysis can be used to identify the individuals and entities involved in BTC transactions. Blockchain analysis companies do this by creating large databases that group BTC transactions into "clusters" through the examination of the data underlying the BTC transactions. As a result, law enforcement can utilize third-party blockchain analysis software to locate BTC addresses that transact at the same time (i.e., the blockchain logs transactions at the same time by two different BTC addresses) and then "cluster" these addresses together to represent the same owner. The third-party blockchain analysis software has supported many investigations and has been found to be reliable.

Id. at *6-7 (internal citations omitted). The only support the magistrate offered for the final assertion—that blockchain analysis software has supported many investigations and has been found to be reliable—was *Gratkowski*. *Id.* at 7, n.6. Of course, the *Franks* and *Daubert* standards are different and apply at different parts of the criminal justice process, but the magistrate's unquestioning acceptance of the reliability of blockchain analysis and a passing reference to *Gratkowski* ignores the serious concerns with the technology. The magistrate fails to note, for example, that neither it nor law enforcement have examined the "black box" of private blockchain analysis software.

When courts have gone beyond the conclusory statements of law enforcement and *Gratkowski*, their analysis fails to perform the kind of reliability analysis *Daubert* requires before evidence may be presented to a jury at trial. For example, in *Matter of Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956*, No. 20-SC-3310 (ZMF), 2022 WL 406410 (D.D.C. Feb. 8, 2022), a magistrate judge questioned the government's search warrant application and whether it complied with the Fourth Amendment. Relevant to this motion, the magistrate asked whether "the software the government used to establish probable cause was reliable." *Id.* at *1. The court engaged in a far more detailed analysis of both Bitcoin and blockchain analysis than other courts, citing a more diverse and complete range of sources, including not only *Gratkowski*, but also other cases that relied on blockchain analysis and the groundbreaking academic work of Professor Sarah Meiklejohn and others. *Id*. at *1-3, *11-*13; *In re the Search of One Address in Washington, D.C. Under Rule 41*, 512 F.Supp.3d 23, 26 (D.D.C. 2021); Sarah Meiklejohn et al, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, IMC '13: Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Oct. 23-25, 2013, at 1, 1 available at https://doi.org/10.1145/2504730.2504747. Throughout the opinion, the court referenced the Pelker article noted above. The court quoted Pelker to say, "there are no published decisions analyzing the weight or reliability of blockchain evidence in a search warrant application" and then adds "not until now." *Id.* at *12.

To assess blockchain forensics' reliability, the magistrate in *Email Accts.* analogized to confidential informants and put great weight on purported prior successes. *Id*. Perhaps because this was a probable cause search warrant evaluation, not a *Daubert* hearing, the court did not look to what the academic and scientific community had to say, but rather what law enforcement alleged. Thus, for example, the court approvingly noted the government's affidavit that "[t]hrough numerous unrelated investigations, law enforcement has found the information provided by these [blockchain forensics] companies to be reliable" and that "this software has correctly analyzed data on the blockchain in hundreds of investigations." *Id*. at *13. It added, "success in the hundreds, with a perfect record in one case as corroborated by 50 search warrant returns, makes this clustering software one of the most reliable bases for a search ever. Going 50 for 50 is beyond what could be expected of a mere human." *Id*. The magistrate concluded, "[t]he unprecedented rate of prior success, lack of incentive or capacity to lie, and incredible level of detail (the software draws out each transaction block-by-block that comprises a cluster), make the clustering software a reliable foundation for probable cause that is beyond compare. Moreover, software that makes a mistake will be deleted and never repurchased, ensuring survival of only the fittest software." *Id.* (internal citations omitted). For the magistrate in *Email Accts*., therefore, unchallenged law enforcement claims, and some faith in the effectiveness of the free market, were sufficient to prove reliability. This sort of freeform analysis may suffice for loosely defined probable cause, but it utterly fails what *Daubert* requires.

Blockchain Analysis Does Not Survive a *Daubert* Challenge.

The Supreme Court in *Daubert* offered five factors to determine whether a scientific methodology should be admitted in a courtroom: (1) "whether it can be (and has been) tested," (2) "whether the theory or technique has been subjected to peer review and publication," (3) "the known or potential rate of error," (4) "the existence and maintenance of standards controlling the technique's operation," and (5) "general acceptance." *Daubert*, 509 U.S. at 593-94. As detailed above, in 2015, Luu and Imwinkelried concluded that blockchain forensics did not pass these benchmarks. But has anything changed?

First, while academic researchers and technologists continue to try and test their techniques, many continue to rely on artificial data sets rather than the public blockchain itself. *See, e.g.*, Malte Möser and Arvind Narayanan, *Resurrecting Address Clustering in Bitcoin*, *ArXiv*abs/2107.05749 (2021), at 1-20, available at https://arxiv.org/abs/2107.05749. For those researchers that do test on the public blockchain, they still apply heuristics and other analytical techniques to get a handle on their large data sets. *See, e.g.*, Yousaf et al, *Tracing Transactions Across Cryptocurrency Ledgers*, Proceedings of the 28th USENIX Security Symposium (Aug. 2019) at 3-6, available at https://www.usenix.org/system/files/sec19-yousaf_0.pdf. There is, however, a major distinction between where academic researchers test their work and where the proprietary blockchain analytics companies do it. Just because a technique was tested by an academic researcher does not mean that a private company follows the same methods or uses the same data. Beyond law enforcement's purported claims of the reliability of the methods, outsiders simply have no means of testing, or even examining, the methods of private companies. As two Princeton academics explained in a 2021 article, a "major issue is the lack of ground truth data available to researchers" and although "[b]lockchain intelligence companies might possess manually curated and refined data sets…their techniques and data aren't openly available to researchers." Möser and Narayanan, *supra* at 2. Thus, for all the recent research related to blockchain analysis, testing lacks consistent data sources and private companies' work remains unavailable.

Second, while there has been an outpouring of scholarship related to Bitcoin and other cryptocurrencies in the past decade, much of it peer-reviewed, many questions remain unanswered. *See, e.g.*, Arianna Trozze et al, *Cryptocurrencies and future financial crime*, 11 Crime Science, 1-35 (2022); Yousaf et al, *supra* at 2. One recent paper aptly summarized the field as "still evolving and poorly understood." Natkamon Tovanich et al, *Visualization of Blockchain Data: A Systematic Review*, 27 IEEE Transactions on Visualization and Computer Graphics, 3135 (July 2021). And a paper from 2018, in the *Journal of Forensic Research,* concluded that even the most common type of forensic blockchain analysis developed by Sarah Meiklejohn still had "room for further research." Douglas A. Orr, *Bitcoin Investigations: Evolving Methodologies and Case Studies*, 9 J. Forensic Rsch, at 6 (May 2018), available at https://www.hilarispublisher.com/open-access/bitcoin-investigations-evolving-methodologies-and-case-studies-2157-7145-1000420.pdf. Certainly the proliferation of commercial companies offering blockchain analysis services suggests a faith in the techniques, but commercial acceptance has never been an independent factor under *Daubert*, nor can it be, since proprietary commercial software by definition cannot be peer reviewed. In short, the academic literature has steadily improved since Luu and

Inwinkelried looked at it 2015, but there is still no consensus on the reliability of blockchain analysis.

Third, rates of error in blockchain analysis remain essentially unknown. Scholars have noted, for example, that the heuristics underpinning blockchain forensics are "vulnerable to false positives," especially if users "adopt privacy-enhancing countermeasures." Möser and Narayanan, *supra* at 3, 15. As the two Princeton researchers noted in 2021, "analyses of clustering heuristics often fall short of quantifying their accuracy." *Id*, at 2. Thus, recent scholarship has not resolved Luu and Inwinkelried's 2015 concerns about the high false positive rate and incompleteness of published results. Luu and Imwinkelried, *supra* at 18. These problems are even more pronounced with the proprietary commercial services who, as far as the defense can determine, reveal no details about their own rates of error. Since the government and private firms are unlikely to publicize instances when blockchain analysis proves unreliable, courts should not presume reliability based on successful investigations, like the court did in *In re the Search of One Address in Washington, D.C. Under Rule 41*. Touting the successes tells us nothing about the failures. More than a decade after blockchain analysis emerged, we simply do not know its reliability.

Fourth, operational standards in blockchain analysis have improved, but the same issues of secrecy surround the standards in the commercial realm. So, for example, academic researchers can build on the work of their predecessors, like Möser and Narayanan did with the work of Meiklejohn. Möser and Narayanan, *supra* at 1-20. But blockchain analysis companies like Chainalysis or TRM Forensics do not publicly reveal their standards of operation. Perhaps they disclose more information to paying clients, but courts and defense attorneys are expected to take on faith "the existence and maintenance of standards controlling the technique's operation." *Daubert*, 509 U.S. at 594. In light of the fluidity and dynamism of blockchain technologies and the back-and-forth between those seeking greater privacy and those seeking to unmask transactions, it is unclear whether there can ever be operational standards.

Fifth and finally, blockchain forensics have been used more commonly since Luu and Imwinkelried wrote in 2015, but that does not mean that the reliability of blockchain analysis is generally accepted. The fact that it has been used often in investigations is hardly grounds, alone, to conclude that its reliability is generally accepted. Similarly, the proliferation of commercial blockchain analysis companies suggests there is a market, but the marketability of a service is not the measure of general scientific acceptance. One need only think of snake oil or alchemy to see that point. The growth of the blockchain analysis industry is a sign of growing acceptance, but until their proprietary methods are subject to expert scrutiny, we simply have no way of knowing what sort of general acceptance they deserve.

Conclusion.

The Government says it will introduce export and non-expert testimony at the trial regarding blockchain analysis in this case. The defense asserts that technology is not reliable and will not withstand analysis under the *Daubert* factors. After the Government responds, the court should hold an evidentiary hearing at which the Government is permitted to attempt to show the reliability of blockchain analysis, and the defense is permitted to challenge reliability. Thereafter, the court should find that such evidence is not admissible.

A hearing is requested.

No further memorandum is submitted because all authority necessary to grant this motion is contained herein. However, because some of the cited articles could not be linked and may not be immediately available to the court, those are attached as exhibits to this motion.

WHEREFORE the defense requests that the court hold a hearing on this motion and thereafter grant the motion and bar the Government from offering at trial any expert and non-expert testimony regarding forensic blockchain analysis.

Date: July 29, 2022.

Respectfully submitted,

/s/ Richard Guerriero
Richard Guerriero, Esq.
N.H. Bar ID. 10530
Legal Intern: Oliver Bloom
Lothstein Guerriero, PLLC
Chamberlain Block Building
39 Central Square, Suite 202
Keene, NH 03431
Telephone: (603) 352-5000
richard@nhdefender.com

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to registered participants identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to the nonregistered participants on the date the document was signed by me.

/s/ Richard Guerriero
Richard Guerriero, Esq.