NORTON ROSE FULBRIGHT

Blockchain Law

When blockchain analytics meet the ‘Daubert’ test

Robert A. Schwinger, *New York Law Journal* — July 23, 2024

Even under the 2023 amendment to Rule 702 that attempts to curtail some courts’ overly permissive approaches to ‘Daubert’, recent rulings show that expert blockchain analysis can indeed satisfy the gatekeeping threshold for admissibility in litigation.

Blockchain analysis claims to be able to break through the supposed anonymity of blockchain transactions and identify the individuals involved. But when such analysis is proffered in litigation, can it meet the *Daubert* gatekeeping test for reliable, admissible evidence under Rule 702 of the Federal Rules of Evidence?

Even under the 2023 amendment to Rule 702 that attempts to curtail some courts’ overly permissive approaches to *Daubert*, recent rulings show that expert blockchain analysis can indeed satisfy the gatekeeping threshold for admissibility in litigation.

Introduction

Although for some users part of the appeal of cryptocurrency is its perceived anonymity, the burgeoning blockchain analysis industry offers services that allow both government enforcers and private litigants to trace transactions conducted on the blockchain based on the public-facing information freely available from the blockchain.

Particularly when combined with other sources of information, blockchain analytics can frequently trace transactions back to a real-world user, despite the user’s attempts to conceal their identity. Thus, as characterized by one court, cryptocurrency transactions are “both uniquely anonymous and uniquely public.” *United States v. Sterlingov*, 2024 WL 860983, at *1 (D.D.C. Feb. 29, 2024).

In recent years, blockchain analytics have become an increasingly common tool in prosecuting offenses and litigating disputes involving cryptocurrency and other blockchain transactions. But is this in fact a reliable methodology the courts should be accepting, or is it the kind of “junk science” from which Rule 702 and *Daubert* seek to protect the judicial process?

Requirements under evidence Rule 702

This question arises at a time when there has been renewed emphasis in federal litigation generally on the need to adhere strictly to Rule 702’s requirements. Rule 702 was intended to codify the framework for the admissibility of expert evidence

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US.
Matthew Niss, a litigation associate at the firm, assisted in the preparation of this article.

established by the Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

However, it was recently amended this past December, in part out of concern that that the *Daubert* rulings of "many courts" reflected "an incorrect application of Rule[] 702." 2023 Advisory Committee Note to Fed. R. Evid. 702.

Rule 702 currently provides:

> 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 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.

The 2023 amendments to Rule 702 were intended "to clarify and emphasize that expert testimony may not be admitted unless the proponent demonstrates to the court that it is more likely than not that the proffered testimony meets the admissibility requirements set forth in the rule," 2023 Advisory Committee Note to Fed. R. Evid. 702. Under the amendment, "the critical questions of the sufficiency of an expert's basis, and the application of the expert's methodology," are threshold gatekeeping questions for the court that go to the "admissibility" of the expert evidence altogether, and not merely to how much "weight" it should be given by the trier of fact.

The amendment also sought "to emphasize that each expert opinion must stay within the bounds of what can be concluded from a reliable application of the expert's basis and methodology." 2023 Advisory Committee Note to Fed. R. Evid. 702. The Advisory Committee noted in particular that "the judge should (where possible) receive an estimate of the known or potential rate of error of the methodology employed, based (where appropriate) on studies that reflect how often the method produces accurate results."

These provisions thus raise the question of whether the results of blockchain analysis can be sufficiently reliable to pass muster under *Daubert* and Rule 702. While this column previously discussed certain decisions examining the reliability of blockchain analytics (*see* R. Schwinger, "Anonymous No More: Blockchain Analytics in the Courts", New York Law Journal, May 24, 2022), those earlier cases arose in the context of determining whether search warrant applications were supported by sufficiently reliable information to establish "probable cause."

But the probable cause standard differs materially from the *Daubert* standard. *See, e.g., U.S. v. Pirosko*, 787 F.3d 358, 370 (6th Cir. 2015) (explaining that "we have never held that a search warrant affidavit must always be supported by evidence admissible under *Daubert*."). Recent rulings are now examining this issue under Rule 702 principles that govern expert testimony and evidence in all litigation, civil and criminal.

Overview of blockchain analytics

A recent decision upholding the admission of blockchain analysis evidence under the amended Rule 702, *United States v. Sterlingov*, 2024 WL 860983 (D.D.C. Feb. 29, 2024), provides a good overview of various techniques frequently used in blockchain analysis. These techniques derive from the fact that:

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.

One common analytic technique involves "clustering" cryptocurrency addresses: by analyzing different transactions to associate them with a specific user, blockchain analytics companies are often able to illuminate otherwise anonymous transactions. Although this process could be done manually, given the vast amount of data to be considered blockchain analytics companies employ algorithms and several clustering techniques, or “heuristics,” to analyze the blockchain and attempt to trace transactions of interest.

Perhaps the most well-known heuristic is often referred to as “co-spend,” or common spend. Because a blockchain “transaction can contain multiple input addresses and multiple output addresses…when a transaction contains multiple inputs addresses, the input addresses are said to be co-spending.” Because a sender must have the private key for each of the input addresses, “it is very likely that a single person or entity controls each of the input addresses.” The ability to identify transactions in this manner is not new, and was even noted in the original bitcoin whitepaper.

Other heuristics are used as well. For example, the analytics firm used by the experts in *Sterlingov*, Chainalysis Government Solutions, and its software product “Chainalysis Reactor” also utilized another heuristic, which posits that:

> very 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. 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.

This heuristic involves “track[ing] unique features [of a certain service], such as the size of the data contained in the transaction or the ‘lock time’ (which is a parameter that schedules a minimal time before the blockchain accepts a transaction)” in order to “use these unique characteristics to identify and to cluster addresses involving the same darknet service.”

In addition to analyzing data from the blockchain, blockchain analytics companies also employ a so-called “intelligence-based heuristic,” in which they analyze other information to help trace transactions using digital currencies, including information obtained from sources such as “data leaks, court documents, [] data partnerships, exchanges that share their addresses[], and manual merges due to services changing wallets.” Although not technically a “heuristic” because it looks only at off-chain data, the gathering of such information may also play a role in the blockchain analysis where it appears useful.

Do blockchain analytics satisfy ‘*Daubert*’?

In *Sterlingov*, the U.S. District Court for the District of Columbia recently rejected a challenge under *Daubert* and Rule 702 to the opinions of two experts who had employed blockchain analysis. The defendant in *Sterlingov was* “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.”

The government proffered two expert witnesses, one from the FBI and the other from Chainalysis, who both addressed the blockchain analytics software Chainalysis Reactor, detailing how Chainalysis Reactor traced hundreds of millions of dollars in bitcoin transactions to the defendant’s mixer, Bitcoin Fog, and also concluded that several darknet market sites had sent and received millions in bitcoin from Bitcoin Fog.

The defendant argued that Chainalysis Reactor, and these experts’ use of it, could not satisfy Rule 702 and the *Daubert* factors, claiming that its heuristics had not been peer reviewed and that its rate of false positives was unreported, thereby rendering it inadmissible under Rule 702(c) for not being “the product of reliable principles and methods.”

After holding a series of *Daubert* hearings, the court rejected this argument. In a detailed technical discussion, the court found that the software “easily clears the threshold for reliability, and thus admissibility.”

First, both experts were experienced in using blockchain analytics for investigations and testified that based on their “real-world experience,” the software was “highly reliable.” Their experience included work as part of the U.S. Department of Justice’s National Cryptocurrency Enforcement Team, with the FBI, with the Drug Enforcement Administration, and with Chainalysis itself. One expert testified that she was unaware of a “single false positive” resulting from the software, and that, if anything, its analysis was “underinclusive” because of Chainalysis’s “conservative approach to clustering.”

The court also found that reliability of the Chainalysis Reactor software was reinforced by other corroborating evidence. For example, the FBI conducted “sting transactions” with the bitcoin mixer at issue and, through a by-hand analysis, attributed five addresses to the mixer. Of these addresses, Chainalysis Reactor correctly identified four of the five addresses, and did not include the fifth due to its conservate approach.

The court also found that the defendant's own evidence supported the reliability of Chainalysis Reactor, because the defendant's expert, who was employed by another blockchain analysis company, agreed that the "co-spend" heuristic was "highly reliable." Although this expert testified that Chainalysis Reactor's analysis of the second heuristic involving behavioral patterns that amount to a digital fingerprint was "error-prone," the court found this testimony dubious because this expert's employer was currently developing its own competing version of this heuristic. The court further noted that the "intelligence" heuristic was only used in a "very limited capacity" in the experts' analysis.

The court thus explained that the Chainalysis Reactor software satisfied all of the *Daubert* factors:

- The first *Daubert* factor ("whether the theory or technique can be and has been tested") was satisfied because both the prosecution and defense experts had been able to largely replicate the results produced by Chainalysis Reactor.
- The second *Daubert* factor ("peer review and publication") was met because the "co-spend heuristic has received widespread academic approval," even if not subject to a traditional academic peer review process.
- The third *Daubert* factor ("the method's known or potential rate of error") was found to pose no bar to admissibility. Although Chainalysis did not record the software's rate of false positives or negatives, this factor was satisfied by the expert testimony on the use of confirmatory "sting transactions," and because the software's results were confirmed by analysis done using the software of another blockchain analytics company, and the analysis by the defense's expert.
- Finally, the fourth *Daubert* factor ("whether the theory or technique finds general acceptance in the relevant scientific community") was satisfied because of the evidence that "blockchain tracing…is widely relied upon by both the law enforcement and business communities," and that Chainalysis "in particular is viewed as an industry standard tool."

Accordingly, the court found "by a preponderance of the evidence" that "the government's blockchain tracing evidence readily clears the hurdle necessary" for expert evidence to be admissible and presented to the jury under Rule 702 and *Daubert*.

Other recent decisions finding blockchain analytics evidence admissible under Rule 702

The *Sterlingov* decision was notable for its detailed discussion and analysis of blockchain analysis techniques. But other recent court decisions have also upheld the admission of expert testimony on blockchain analysis under *Daubert*, though at less length and detail than in *Sterlingov*.

In the U.S. Court of Appeals for the First Circuit earlier this year, for example, the court upheld the trial court's admission of evidence from an expert from the blockchain analytics firm CipherTrace, who used blockchain analysis to show that the My Big Coin cryptocurrency that the defendant had promoted was not actually associated with any public blockchain, in contrast to the defendant's statements otherwise. *United States v. Crater*, 93 F.4th 581 (1st Cir. 2024). The defendant was subsequently convicted of wire fraud, unlawful monetary transactions, and "operating an unlicensed money transmitting business based on his involvement in a cryptocurrency scheme."

The defendant argued on appeal that the expert's testimony should have been excluded on the grounds that (1) she was not sufficiently qualified by education to serve as an expert witness because she did not hold a computer science degree, (2) her opinions were not "based on sufficient facts or data" and her proposed testimony was not "the product of reliable principles and methods," and (3) the district court failed to conduct a formal *Daubert* hearing before admitting her testimony.

The First Circuit rejected each of these arguments and upheld defendant's conviction.

Addressing the defendants' three principal objections on appeal, the First Circuit affirmed the trial court's conclusion that the expert's lack of a computer science degree did not make her "unfit to opine as an expert," because she was qualified by "extensive professional experience in blockchain investigations." Specifically:

> In addition to her work as the Director of Financial Investigations and Education for CipherTrace, she had created multiple training courses, conducted trainings for Interpol, Europol, and the United States Departments of Treasury, Homeland Security, and Justice, authored articles, and lectured at conferences and universities on blockchain technology and cryptocurrency investigations.

The defendant's second argument about the expert's methodology or its reliability was likewise rejected, because the defendant failed to identify any "facts, data, methods, or principles" employed by the expert that supposedly were objectionable. Moreover, defendant's own expert had "agreed that CipherTrace's blockchain analysis could 'reveal a number of details of [a] system and its contents.'"

Finally, the court "disagree[d] with [the defendant] that the district court abdicated its gatekeeping function by resolving his…objections to [the expert's] testimony without holding a *Daubert* hearing." The court cited First Circuit precedent that "[t]here is no particular procedure that the trial court is required to follow in executing [the *Daubert*] gatekeeping function," and stated that First Circuit had "specifically rejected the argument that a district court must necessarily hold [a *Daubert*] evidentiary hearing." Moreover, the defendant "does not explain what more a *Daubert* hearing could have accomplished with regard to these inquiries."

The court also noted that while no formal *Daubert* evidentiary hearing was held, the trial court did hold "oral argument at the final pretrial conference" on the defendant's motion to exclude the expert. Defendant there argued that the expert's testimony risked confusing the jury because her opinion was "limited to public blockchains" and thus "did not sufficiently allow for the possibility that the defendant's cryptocurrency was associated with a private blockchain during the relevant time."

However, the trial court concluded that this argument presented no "reason to exclude [the expert's] testimony in its entirety" but rather simply raised "'fertile ground' for cross-examination."

Accordingly, the judgment of conviction was affirmed over the *Daubert* challenge to the expert's testimony.

Other recent decisions reinforce that blockchain analytics can be reliable, admissible expert evidence. In *SEC v. Balina*, 2023 WL 8040767 (W.D. Tex. Nov. 20, 2023), decided just days before the Rule 702 amendments came in to effect, the court denied a *Daubert* motion seeking to exclude expert's opinions that were partly based on blockchain analysis.

The expert was a Ph.D. business school professor at Wharton who was assisted by a forensic data analytics and litigation consulting firm. He opined on whether the defendant controlled the investment pool for a particular coin and its smart contract, based on records available from the Ethereum blockchain, collecting transaction details, and matching and comparing them to the contents of documents and a database allegedly used by the defendant.

In upholding the expert testimony, the court stated:

> The court finds that the methods used by [the expert] to cross-check public information and information provided by the SEC are sufficiently reliable because [the defendant's] Ethereum address is undisputed and the record of transactions made on the Ethereum blockchain is immutable, enabling the analysis of past transactions with a high degree of confidence that they actually occurred (quotations omitted).

The court also rejected arguments that it was improper for the expert to (1) rely on certain parts of the data analysis performed for him by the consulting firm, (2) include some opinions relating to the limitations of the data, and (3) provide background information about relevant terminology used in this specialized area.

Of some note also is *United States v. Arcaro*, 2024 WL 40213 (S.D. Cal. Jan. 3, 2024), decided earlier this year, where the FBI used "blockchain analysis" to vet claims for restitution in connection with the forfeiture obtained from the defendant as a result of his criminal conviction in a scheme to defraud investors on the cryptocurrency platform BitConnect.

While this proceeding did not involve a *Daubert* challenge or assertion of any other Rule 702 issues, the court nevertheless found that "the vetting process utilized a reasonable and reliable methodology to determine the viability of the third-party claims." The process had consisted of "FBI agents determining whether a potential victim could provide proof that he/she sent money from a cryptocurrency wallet they controlled to a BitConnect wallet." As no one had "lodged a valid objection to the vetting process…[t]he court therefore accepts the results of the government's vetting process."

Not all blockchain analytics experts make the cut

Nevertheless, not every proffer of expert testimony relying on blockchain analysis has succeeded under the *Daubert* test. In *SEC v. Terraform Labs*, 2023 WL 8944860, at *11 (S.D.N.Y. Dec. 28, 2023), the court granted a motion to exclude such expert testimony because the expert "ha[d] not demonstrated sufficient expertise in blockchain analysis," where he "could not name any specific tools he had used in his professional experience to review blockchain transactions and, even more strikingly, admitted that he did not personally analyze the Terraform blockchain data."

Moreover, "the analysis discussed in [the expert]'s report was performed by employees of the consulting firm Cornerstone Research, whose qualifications or methodology [the expert] did not know at all. Nor could [the expert] even recall which computer program the Cornerstone analysts had used."

But notably, the exclusion of this evidence related to the expert witness's lack of experience with blockchain analytics software and direct involvement in the analysis, and not on any claim of unreliability of blockchain analytics in itself.

Conclusion

Decisions like *Sterlingov* and *Crater* upholding under *Daubert* the admission of expert testimony based on the use of blockchain analytics add to a growing body of case law recognizing the reliability of blockchain analytics software, particularly where industry-standard software is used by well-qualified expert witnesses. Future litigants may still challenge the use of blockchain analytics software or other methods of analysis, particularly if it involves the use of different or novel heuristics, or is propounded by an inexperienced expert, as in the *Terraform Labs* decision.

However, as courts increasingly accept these techniques as reliable, challenges to the use of blockchain analytics software or other blockchain analysis techniques in and of themselves may prove difficult to sustain.

NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across more than 50 locations worldwide, including Houston, New York, London, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg, covering the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com

Norton Rose Fulbright Verein, a Swiss verein, helps coordinate the activities of Norton Rose Fulbright members but does not itself provide legal services to clients. Norton Rose Fulbright has offices in more than 50 cities worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg. For more information, see nortonrosefulbright.com/legal-notices. The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.