NORTON ROSE FULBRIGHT

Blockchain Law

Anonymous no more: Blockchain analytics in the courts

Robert A. Schwinger, *New York Law Journal* — May 24, 2022

Blockchain transactions are often said to be anonymous or at least pseudonymous—but are they really? At least for some users, part of the appeal of using cryptocurrency is the perceived anonymity it seemingly offers. But increasingly, judicial decisions and governmental enforcement activity show that this perception is mistaken.

A burgeoning industry of blockchain analysis tools now enables governments and litigants to analyze cryptocurrency transactions on the blockchain and in many cases trace them back to an identifiable, real-world user, even where such users have taken steps to conceal their identity. Recent developments show how courts and enforcers have embraced using this technology.

The problem of anonymity

As this column has previously noted, the government has identified the anonymity and obfuscation of identities in blockchain transactions as a key challenge in proceeding against wrongdoers who make use of that technology. See R. Schwinger, *DOJ's 'Cryptocurrency Enforcement Framework'*, NYLJ (Jan. 15, 2020). An October 2020 report of the Attorney General's Cyber-Digital Task Force on their "Cryptocurrency Enforcement Framework" stated that "[g]iven the complexity of cryptocurrency technology and of the platforms on which it is used, law enforcement professionals across agencies must continually … employ the many appropriate legal tools available to bring individuals and entities that abuse cryptocurrency to justice." Report at 45.

The report included as an accompanying graphic (id. at 48, Fig. 18) a complex diagram of transactions titled "Example of an Illicit Transaction Path Developed Through Blockchain Analysis" that was taken from the government's forfeiture complaint in *U.S. v. 280 Virtual Currency Accounts*, Civ. No. 20-2396 (D.D.C. Aug. 27, 2020), which arose from two hacks of virtual currency exchanges by North Korean actors. The report noted that "[s]uccessful investigations of such schemes require enhanced training and technical capabilities," id., such as using blockchain analysis to uncover real-world identities.

What is 'Blockchain Analysis'?

Blockchain analysis services or analytics allow law enforcement agencies and others to identify the individuals behind illicit or challenged transactions. A recently unsealed magistrate judge memorandum opinion in *In re Search of Multiple Email Accounts Pursuant to 18 U.S.C. §2703 for Investigation of Violation of 18 U.S.C. §1956 et al.*, 2022 WL 406410 (D.D.C. Aug. 26, 2021,

Robert A. Schwinger *is a partner in the commercial litigation group at Norton Rose Fulbright US.*

Matthew Niss, *an associate in the firm's regulation, investigations, securities, and compliance group, assisted in the preparation of this article.*

More than 50 locations, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg.

released Feb. 8, 2022), that was issued in connection with a search warrant application regarding a Bitcoin hack, discusses some of these techniques and concludes that they furnish reliable evidence for judicial purposes.

In re Search arose from an August 2016 "remote access trojan" attack that was able to breach a cryptocurrency exchange's security systems, infiltrate its network, and locate private keys that controlled virtual currency wallets. The hackers were able to initiate thousands of unauthorized Bitcoin transactions, resulting in nearly 120,000 Bitcoins being transferred to outside wallets controlled by the hackers. But by using "clustering software," the government was able to trace these funds to various accounts, for which the government now sought a search warrant in order to follow the money trail.

The court explained:

> Cryptocurrency transactions that occur on a blockchain are, by design, publicly available, and thus are pseudoanonymous. Ironically, the public nature of the blockchain makes it exponentially easier to follow the flow of cryptocurrency over fiat funds. Repeated government seizures and forfeiture actions should disabuse the uninformed of the myth that [Bitcoin] is untraceable, yet this myth abides. Indeed, the IRS alone seized $1.2 billion worth of cryptocurrency in fiscal year 2021.

(Citations and quotations omitted.) This is because the various "anonymizing techniques" that wrongdoers often employ "fail when pitted against algorithms that analyze transactions on the blockchain."

The court provided some elaboration on what these algorithmic techniques may consist of. "The most effective algorithms," it said, "employ a technique described as 'clustering.'"

> Essentially, clustering tools rapidly scan the blockchain, which is an enormous data set, to conduct various forms of pattern recognition. As a rudimentary example, an algorithm might discover that a single address on the blockchain receives the same quantity of [Bitcoin] at regular time intervals. Those seemingly unrelated addresses would then be clustered together to demonstrate common ownership. The clustering analysis un-mixes, un-tumbles, and de-anonymizes, leaving bare the transactions which illicit actors tried to cover up.

According to the court, such tools are not hard to find:

> There are multiple publicly available tools that enable clustering analysis. These are available for free as open source software and for a fee by private software companies. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions.

The court's discussion was similar to that set forth in the government's forfeiture complaint in *U.S. v. 280 Virtual Currency Accounts*, which stated:

> While the identity of a [cryptocurrency] address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can identify the owner of a particular [cryptocurrency] address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity.

The government's complaint then provided the following example:

> [A] user or business may create many [cryptocurrency] addresses to receive payments from different customers. When the user wants to transact the [cryptocurrency] that it has received (for example, to exchange [that cryptocurrency] for other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain analysis companies to investigate virtual currency transactions.

How does it work?

> These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying the virtual currency transactions.

Does Blockchain Analysis Stand Up in Court?

The recently-released ruling in *In re Search* voiced full-throated support for looking to blockchain analysis services to provide reliable evidence that can support critical judicial determinations, such as the probable cause determinations needed for the issuance of search warrants. *In re Search* provides a detailed discussion adding to the nascent but growing body of case law recognizing blockchain analysis software as a reliable tool that law enforcement can use to further its investigations and prosecutions—and that private litigants might be able to utilize in appropriate circumstances as well.

In re Search documented the reasoning of U.S. Magistrate Judge Zia Faruqui in granting the government's application for a warrant to search certain email accounts. Those accounts were controlled by the suspected hackers of a cryptocurrency exchange, from which the misappropriated Bitcoin had been routed through a byzantine web of transactions to various accounts and wallets the hackers controlled.

Using blockchain analysis "clustering" software, the government was able to trace these transactions and follow the flow of money to the email accounts for which the warrant was sought. It did this by analyzing the publicly-available transactions stored on the blockchain, conducting various forms of pattern recognition, and thus demonstrating the common ownership of nominally unrelated blockchain addresses.

In assessing the government's application for a warrant, the court analyzed, among other issues, whether the government's collection of evidence through blockchain analysis software complied with the Fourth Amendment's protections against unreasonable searches and seizures, and whether the software constituted a reliable basis on which the government could establish probable cause. While the court noted that until this decision there were "no published decisions analyzing the weight or reliability of blockchain evidence in a search warrant application" (quoting C. Alden Pelker et al., *Using Blockchain Analysis from Investigation to Trial*, 69 DOJ J. Fed. L. & Prac. 59, 68 (2021)), it concluded that the government's showing in this case satisfied both requirements.

The court first held that the government's use of blockchain analysis software did not contravene the Fourth Amendment's proscriptions against unreasonable searches and seizures. Following the U.S. Court of Appeals for the Fifth Circuit's earlier decision in *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020) (discussed in R. Schwinger, *A Little Less Privacy: Cryptocurrency Transactions Under the Fourth Amendment*, NYLJ (July 27, 2020)), *In re Search* held that a "search" only occurs where a person has a "reasonable expectation of privacy," but that no such reasonable expectation exists where the information at issue was voluntarily turned over by the user to third parties.

Central to the decisions of both courts was that transferring cryptocurrency involved a voluntary act (i.e., conducting a transaction using cryptocurrency), and that cryptocurrency users are "unlikely to expect that the information published on the Bitcoin blockchain will be kept private," undercutting any claim to a legitimate expectation of privacy.

The court was unmoved by the possibility that a cryptocurrency "novice" might "lack the technical savvy or good sense" to know that such information (including addresses and details of cryptocurrency transfers) was publicly available, noting that the public availability of such transactions was "the point of the blockchain." Likewise, it concluded that blockchain analysis software was not an impermissible, warrantless use of technology by the government to circumvent reasonable expectations of privacy, given that such software was available to the public and analyzed publicly-available information stored on the blockchain.

The court next concluded that the blockchain "clustering" analysis was sufficiently reliable that it could be used to establish probable cause. The court characterized clustering software as essentially being a kind of "confidential source in another form," since it "provided law enforcement with the direction of where to look to find suspect transactions and a Rosetta stone to decipher seemingly unrelated transactions."

The court noted, though, that in contrast to the situation presented when relying on the typical informant cited in search warrant applications, i.e., a natural person, it "made little sense" when considering blockchain analysis software for the court to question the "motives or trustworthiness of [the] informant." Nor was there reason to doubt the veracity of the underlying transaction data captured in the blockchain itself, on which the clustering analysis relied, since it is produced by an "automated process," here, the Bitcoin protocol.

Thus, the only question really presented was the reliability of the blockchain clustering software itself. The court addressed this by once again analogizing to how courts assess the reliability of conventional "confidential sources."

The court noted that in cases involving conventional human confidential sources, anywhere from five to eight prior successful tips would typically lead courts to conclude that a proffered source was reliable. The court then compared this to the results of an analysis of clustering software that had been conducted by law enforcement in an unrelated case, which the government had submitted in support of its warrant application.

In that other case, clustering software led law enforcement to 50 customers of a darknet child pornography site, and in all 50 instances the clustering software's analysis was corroborated by the results of further investigation. *In re Search* termed this success rate "unprecedented." The court further noted clustering analysis's "lack of incentive or capacity to lie" and its "incredible level of detail." This, concluded the court, made blockchain analysis software a "reliable foundation for probable cause" that was "beyond compare."

Other Decisions Treating Blockchain Analysis as Reliable

In re Search is notable because it offers what appears to be first comprehensive discussion of the reliability of blockchain cluster analysis software as used by law enforcement. However, other courts have noted the software's reliability, albeit in a more limited manner.

Indeed, Magistrate Judge Faruqui himself issued an opinion a few months before *In re Search* that noted and relied upon blockchain analysis but did not address it in much detail. *In re Search of One Address in Washington, D.C., Under Rule 41*, 512 F. Supp. 3d 23 (D.D.C. 2021). In that case, he approved a pretrial forfeiture of assets whose use was linked to child pornography offenses, noting that "law enforcement can use publicly-available software to analyze the [Bitcoin] blockchain by forensically examining, tracing, and mapping data on the blockchain to unmask the identities of specific users of a given cryptocurrency wallet" (quotations and elisions omitted), and concluded based on that analysis that "[t]here is probable cause to believe the Target Properties have the requisite connection to these alleged crimes."

The Fifth Circuit referenced blockchain analysis software in its 2020 *Gratkowski* decision, 964 F.3d 307, which likewise arose from alleged use of cryptocurrency to purchase child pornography. However, unlike *In re Search, Gratkowski* did not involve approval of a search warrant request because the government served a grand jury subpoena on a cryptocurrency exchange to obtain information about accounts from which funds had been transferred.

The Fifth Circuit explained:

> When an organization creates multiple Bitcoin addresses, it will often combine its Bitcoin addresses into a separate, central Bitcoin address (i.e., a "cluster"). It is possible to identify a "cluster" of Bitcoin addresses held by one organization by analyzing the Bitcoin blockchain's transaction history. Open source tools and private software products can be used to analyze a transaction.

In *Gratkowski*, "[f]ederal agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by" the child pornography website. Then, by seeking through a grand jury subpoena to the cryptocurrency exchange "all information on the [exchange's] customers whose accounts had sent Bitcoin to any of the addresses in the Website's cluster," the defendant was identified as one of these customers. The defendant made no challenge to the reliability of the information the clustering software had produced, but merely raised a Fourth Amendment challenge to the process, which was rejected for reasons similar to those cited in *In re Search*.

Other cases likewise have accepted the results obtained through blockchain analytics. Last year, in *United States v. Dove*, for example, a Magistrate Judge's report and recommendation noted that "third-party blockchain analysis software has supported many investigations and has been found to be reliable," 2020 WL 9172971 (M.D. Fla. Sept. 4, 2020). This report was later adopted by the District Court, which noted that "[a]s a result of numerous unrelated investigations, law enforcement has found the intelligence provided by these third-party companies to be reliable." 2021 WL 838737 (M.D. Fla. March 5, 2021).

In another case last year, *U.S. v. 155 Virtual Currency Assets*, 2021 WL 1340971 (D.D.C. April 9, 2021), the government sought in rem the seizure and forfeiture of cryptocurrency assets that allegedly were involved in transactions designed to support

various terrorist groups. On the government's motion for a default judgment, the court reviewed the government's claimed basis for seeking the forfeiture. The court noted that "[d]espite Bitcoin's pseudonymous nature, law enforcement can sometimes identify parties to a transaction," such as through cluster analysis, and that "[a]uthorities took advantage of third-party blockchain software to perform the investigation here." Based on this showing, the court concluded that the government "has thus established a reasonable basis to believe that the Defendant Properties belonged to entities that provided financial support to [foreign terrorist organizations]."

Still other decisions have accepted the use of blockchain analysis software to establish key facts without substantial analysis or comment. In *United States v. Decker*, 832 F. App'x 639 (11th Cir. 2020), the court affirmed the district court's acceptance of the factual basis for a guilty plea, holding it was not plain error where such basis included, among other things, use of blockchain analysis to reveal that defendant's cryptocurrency transactions "originated from dark net markets."

Similarly, in a challenge to pretrial detention in the prosecution of a bitcoin mixing service's alleged operator, the court accepted "the government's blockchain analysis" without question or extensive analysis to connect the defendant to millions of dollars in transactions with "known darknet markets." *U.S. v. Sterlingov*, 2021 WL 5275702 (D.D.C. Nov. 10, 2021).

On the civil side, *Gadasalli v. Bulasa*, 2022 WL 991993 (E.D. Tex. April 1, 2022), was a civil action brought by a plaintiff who met the defendant on a dating site and claimed that the defendant defrauded her in various cash-for-cryptocurrency swindles. In its recitation of facts submitted in support of plaintiff's ex parte motion for a temporary restraining order freezing certain of defendant's cryptocurrency and cryptocurrency accounts, the court noted without issue that "blockchain analytics successfully traced Gadasalli's funds to cryptocurrency wallet addresses under Bulasa's control," although the court ultimately denied the requested relief on other grounds.

In another recent civil case, *Strivelli v. Doe*, 2022 WL 1082638 (D.N.J. April 11, 2022), the plaintiff's cryptocurrency and other digital assets were stolen by an anonymous hacker whom he met solely online. Although the plaintiff never learned the alleged thief's name, the plaintiff retained a blockchain analytics firm that traced the stolen assets through multiple other wallets, some of which were hosted by cryptocurrency exchanges with "know your customer" obligations, who thus would be expected to retain the alleged thief's identity.

After the plaintiff filed a "John Doe" complaint against the thief, the court granted plaintiff's ex parte motion for expedited discovery from those exchanges so that the plaintiff could identify and serve the anonymous defendant with the complaint. The court noted that the requested discovery was not unreasonable since plaintiff "provided compelling evidence that traces his stolen assets to wallets and transactions on the Exchanges" in the form of a blockchain analytics report.

Conclusion

In re Search quoted from the 1998 Coen brothers cult classic film "The Big Lebowski" to state as its conclusion: "Cryptocurrency and related software analytics tools are '[t]he wave of the future, Dude. One hundred percent electronic.'" The court may well be right. In a short period of time, decisions by numerous courts have concurred that blockchain clustering analysis is a reliable form of evidence that can be used to trace the flows of cryptocurrency.

Prudence thus dictates that cryptocurrency users disabuse themselves of the notion that their transactions are anonymous or otherwise private. Private litigants and criminal defendants should be aware that blockchain analysis software can effectively trace transactions on the blockchain, and is widely available to both the public and law enforcement. Moreover, in light of the growing body of case law accepting use of such analysis, parties are likely to face an uphill battle to prevent its use in future disputes.