First Annual Dennis Karjala Memorial Workshop

Blockchain in the Courts

Daniel J. Neally | Maria L. Hodge[1]

Center for Law, Science and Innovation
Sandra Day O'Connor College of Law
Arizona State University

Held November 3, 2018
at the Beus Center for Law and Society
Phoenix, Arizona

[1] Daniel J. Neally, JD Candidate at the Sandra Day O'Connor College of Law, Class of 2019, Center Scholar with the Center for Law, Science and Innovation; Maria L. Hodge, JD Candidate at the Sandra Day O'Connor College of Law, Class of 2021.

The Center for Law, Science and Innovation

The Center for Law, Science and Innovation has been an established leader for over 30 years in addressing the extraordinary legal and regulatory problems caused by rapid developments in science and technology. The Sandra Day O'Connor College of Law at Arizona State University was the first in the country to create a center to address these challenges. As technology increasingly assumes a central role in our lives, the center is uniquely positioned to be an innovator and leader in the teaching and application of 21st century law and policy.

The Dennis Karjala Memorial Workshop

The Center for Law, Science and Innovation hosted with great appreciation the First Annual Dennis Karjala Memorial Workshop on November 3, 2018 at the Beus Center for Law and Society in Phoenix, Arizona. This workshop honors passionate scholar, longtime faculty fellow, and friend of the center Professor Dennis Karjala, who passed away in 2017. Dennis enjoyed organizing events focused on the latest issues at the intersection of technology and the law. Each year, the Dennis Karjala Memorial Workshop will feature discussions on cutting-edge issues in innovation governance and emerging technology.

This year's theme was Blockchain in the Courts. This invitation-only workshop included presentations on and wide-ranging discussions of the use and regulation of blockchain technology. Participants discussed existing and future frameworks for the governance of blockchain applications, the legal and practical challenges bearing on discovery and admissibility of blockchain evidence, and potential governmental uses for blockchain technology.

This report describes the engaging presentations and discussions that took place at the workshop. This report is intended to capture the presentations and discussions from the day of the workshop. This is not a consensus document. The opinions, recommendations, and conclusions included in this report were captured during roundtable discussions and do not necessarily reflect the views of all participants or their affiliated institutions.

Table of Contents

Workshop Agenda

8:30-8:45	*Workshop Welcome, Objectives and Introductions* Gary Marchant, Sandra Day O’Connor College of Law, ASU
8:45-9:15	*Blockchain in Government: A Key Tool to Prevent Cyber Threats* John Zanni, President, Acronis
9:15-9:45	*Use Case of a Blockchain-Based Common Identity System and Proof of Existence* David Berger, Chief Technology Officer, Integra
9:45-10:00	Discussion
10:15-10:45	*Justice Use Cases for Blockchain: Opportunities and Challenges* Paul Embley & Diana Graski, National Center for State Courts; Anne Thompson, Thomson Reuters
10:45-11:15	*Evidence in Smart Contract Dispute Resolution: Where Theory Meets Reality* Carla Reyes, Michigan State University College of Law
11:15-11:30	Discussion
11:30-12:00	*Providing a Legal Framework for Blockchain Activities – And a Blockchain Framework for Legal Activities* Oliver Goodenough, Vermont Law School
12:00- 12:30	*Admissibility of Blockchain Evidence* Grant Autrey and Gary Marchant, ASU College of Law
12:30-1:00	*"Discovering" Blockchain Evidence* Antigone Peyton, Protorae Law PLLC
1:00-1:15	Discussion

Participants

Josh Abbott	Director, Center for Law, Science and Innovation
Michael Arkfeld	Arkfeld & Associates | Arizona State University
Grant Autrey	JD Candidate, Sandra Day O'Connor College of Law
David Berger	CTO, Integra
Dan Bodansky	Professor, Sandra Day O'Connor College of Law
Jay Carpenter	Desert Blockchain
Shawnna Hoffman-Childress	Global Cognitive Legal Co-Leader, IBM
Larry Cohen	Cohen Law Firm | Arizona State University
Paul Embley	National Center for State Courts
AJ Gilman	J.D. Candidate, Sandra Day O'Connor College of Law
Oliver Goodenough	Professor, Vermont Law School
Diana Graski	National Center for State Courts
Trent Hoffman	JD Candidate, Sandra Day O'Connor College of Law
Kaylee Hoffner	JD Candidate, Sandra Day O'Connor College of Law
Maria Hodge	JD Candidate, Sandra Day O'Connor College of Law
Peter Krehbiel	Associate, Snell & Wilmer LLP
Gary Marchant	Faculty Director, Center for Law, Science and Innovation
Daniel Neally	JD Candidate, Sandra Day O'Connor College of Law
Antigone Peyton	Member, Protorae Law PLLC
Carla Reyes	Assistant Professor, Michigan State University
Aileen Schultz	Principal, Fractal Scale Inc.
Anne Thompson	Thomson Reuters
John Tredennick	Chairman, Catalyst Repository Systems
David Weiss	Arizona State University
John Zanni	President, Acronis

Blockchain applications are poised to become foundational technologies underlying international supply chains, smart contracts, personal identification systems, secure voting, portable personal health data, revolutionized energy markets, and a wide variety of cryptocurrencies. Similarly, blockchain technology is quickly finding its way into legal practice and the courts.

How will legal practitioners, courts, and other public institutions use and regulate blockchain technology? Presenters and participants discussed current examples of blockchain applications being explored and implemented by governments around the world; the merits of self-governance vs. enabling-focused government regulation on the use of blockchain technology; how to conceptualize blockchain technology as not just a fancy database, but a system of trust; and how legal practitioners and the courts will handle the discovery and admissibility of blockchain evidence.

I. Governmental Use of Blockchain Technology

Following an introduction by the Center for Law, Science and Innovation's Faculty Director, Gary Marchant, the President of Acronis, John Zanni, made the first presentation on blockchain applications in government. Zanni gave a brief introduction of his company and its newly created product, Acronis Notary Cloud, which uses blockchain technology for notarizing documents. This product was created to satisfy an untapped market for blockchain applications in government and the legal industry. Market surveys show that the global blockchain industry is expected to grow over forty percent per year for at least the next five years. Several national governments are already beginning to implement this technology.

Estonia

- Among the first countries to adopt blockchain technology
- Used in registries for national health, legislative, judicial, and commercial code systems
- Planning to extend blockchain use to personal medicine, cybersecurity, and data embassies

United States

- Over thirty blockchain initiatives at federal and state levels
- Birth registry and identification system (Illinois)
- Private blockchain for online voting (Utah)
- "Smart records" for public archives and corporate filings (Delaware)

China

- Plans to establish national blockchain standards by 2019
- Highest number of blockchain patents
- Blockchain-backed asset-backed securities on Shanghai Securities Exchange[2]
- First out-of-hospital prescription circulation service[3]

[2] Song Jingli, *Baidu joins global group to advance blockchain technologies*, CHINA DAILY (Oct. 19, 2017), http://www.chinadaily.com.cn/business/tech/2017-10/19/content_33451931.htm.
[3] Eva Yoo, *Pony Ma announces medical blockchain project in Guangxi*, TECHNODE (Apr. 13, 2018), https://technode.com/2018/04/13/pony-ma-blockchain-guangxi/.

Others

- Brazil intends to move petitions and popular voting onto Ethereum[4]
- Canada is testing Ethereum applications for transparency in government grants[5]
- Switzerland has begun offering digital identification registered on Ethereum[6]
- Chile uses Ethereum to track data and finances related to the energy grid[7]
- Dubai plans to become the first integrated, blockchain-powered city by 2020[8]

Zanni expects that the gradual widespread adoption of blockchain technology by the private sector will correlate with adoption by many of the world's governments in 2020. Governments are already the second largest users of blockchain technology, behind banking and capital markets. Eventually, industries may be required to incorporate blockchain to stay relevant in a swiftly changing landscape.

Governmental uses of blockchain come with potential for abuse. For example, Russia is using blockchain to develop and expand ransomware capabilities[9] and other disruptive forms of cyber technology. Zanni noted that programmers developing blockchain products for governments will need to be mindful of security and costs. He believes that many of the concerns currently surrounding government use of blockchain technologies will be addressed as the performance of blockchain applications improves and as the technology becomes more widely adopted in other sectors, including banking and retail.

II. Blockchain Use Cases

David Berger, Chief Technology Officer for Integra, argued that if we can get past certain misconceptions about blockchain, there are many beneficial use cases for the technology. According to Berger, "blockchain" has become an overloaded terms, having been ascribed so many meanings it can be difficult to understand. Lack of precision in how we describe the technology has led to misconceptions about what blockchain is and what it can do.

One such misconception is the idea that blockchain is merely a mediocre database technology. Rather, according to Berger, blockchain should be seen as a system of trust, developed using modern cryptography techniques, which should only be used to store the minimum amount of information necessary for any application. Berger suggested that, to avoid misconceptions, discussions of blockchain be kept simple and, if possible, include a standard definition. He said the best approach, however, would be to focus instead on what the technology can accomplish.

[4] Joseph Young, *Brazilian Government Plans to Process Petitions and Write Laws on Ethereum*, COINTELEGRAPH (Jan. 6, 2018), https://cointelegraph.com/news/brazilian-government-plans-to-process-petitions-and-write-laws-on-ethereum.

[5] Jeremy Nation, *Canada Leverages Ethereum Blockchain for Public Transparency of Government Grants*, ETHNEWS (Jan. 22, 2018), https://www.ethnews.com/canada-leverages-ethereum-blockchain-for-public-transparency-of-government-grant.

[6] Paul Kohlhass, *Zug ID: Exploring the First Publicly Verified Blockchain Identity*, MEDIUM/UPORT (Dec. 6, 2017), https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702.

[7] David Floyd, *Chile is Using Ethereum's Blockchain to Track Energy Data*, COINDESK (Apr. 9, 2018), https://www.coindesk.com/chile-to-use-ethereums-blockchain-to-track-energy-data.

[8] Smart Dubai, *Blockchain Strategy*, https://smartdubai.ae/initiatives/blockchain.

[9] Cory Doctorow, *The True Story of Notpetya: a Russian Cyberweapon that Escaped and did $10B in Worldwide Damage*, BOINGBOING (Aug. 22, 2018), https://boingboing.net/2018/08/22/andy-greenberg.html.

Berger then discussed a variety of use cases for blockchain technology. Blockchain can be used to improve identification services. Few agreed-upon systems currently exist for identifying commodities and products, one example being the International Standard Book Number (ISBN) system for identifying books. Blockchain technology can be used to develop and track other identifiers and create more uniform and trusted standards for keeping track of different goods.

Blockchain could also be used in various business or software tracking systems. Because the technology provides a secure way to verify data, it can be used to reduce fraud among process managers. It can also be used a means of version control for software. Users could more efficiently track changes and verify whether systems are up to date. Finally, blockchain could provide a more organized and agreed upon method for tracking public key registries. According to Berger, these are just a few of the possible uses for blockchain technology.

III. Justice Use Cases for Blockchain

Three presenters participated on a panel discussing possible outcomes for blockchain use in the court system: Paul Embley, Chief Information Officer and Technology Division Director with the National Center for State Courts (NCSC); Diana Graski, a consultant with NCSC; and Anne Thompson from Thomson Reuters.

According to Embley and Graski, blockchain applications have strong potential in this area, but fulfilling that potential will require the education of judges and widespread use by law enforcement officers and legal practitioners. The presenters identified two topics of interest: the issue of jurisdiction over cases involving blockchain and the enforceability of court orders against a platform built for security and anonymity. In the case of jurisdiction, it is questionable whether traditional concepts and rules can be applied because of the distributed nature of many blockchain applications. Physical location is, by the nature of the technology, pervasive and undetermined. This may make it harder to establish contacts and define jurisdiction. Courts will also need to decide how to enforce discovery of blockchain assets and whether disclosure of money in the form of cryptocurrency is limited to its current state or the ledger of all past transactions.

Judges will also need to understand the fundamentals of blockchain technology, as well as the functioning of specific blockchain applications. Uses of the technology may become widespread and could impact digital assets, law enforcement, storage of criminal records, and the condensing of government data. One problem identified during the discussion was the issue of expungement in blockchain applications. Our current model for expunging records is based on the ability to destroy or seal a record completely, but that may not be possible in a world where criminal records and court proceedings are stored using blockchain.

Next, Thompson presented on legislative issues being considered by the NCSC. While legislative efforts have increased in the past year, they are still falling short of what is needed to address the problems presented by blockchain. Proposed policies often rely on limited or outdated definitions, and adopted policies are often inadequate or are slow to be adopted by other states. Some states, including Arizona and

Illinois, have taken a sandbox approach to encourage the development of blockchain applications, but that has not been widely adopted across the United States.

IV. Evidence in Smart Contract Dispute Resolution

Carla Reyes, Professor of Law at Michigan State University College of Law, presented on "smart contracts." A major problem she pointed out is that lawyers generally do not understand what a smart contract is and that the term does not refer to a contract as defined by law. Attempts to apply contract law muddy the waters and create additional problems.

Rather than thinking of a smart contract as a new form of the traditional contract, she suggested viewing a smart contract as just an automated performance of an agreed-upon action based on whether a particular condition occurs—if X happens, then execute Y. Smart contracts are suitable for simple transactions that can be executed without much difficulty, such as escrow. The use of smart contracts should not require a change to modern contract law. They are simply a new tool for the enforcement of contracts and simple transactions.

Reyes explained how placing a smart contract on a blockchain does not change our analysis. Blockchain, as an open and immutable ledger, would merely allow for tracking state changes in a contract. Nothing about the blockchain changes the actual contract, smart or otherwise. Therefore, concerns about applying the technology in contracting are purely hypothetical.

V. Legal Framework for Blockchain Activities; Blockchain Framework for Legal Activities

Oliver Goodenough, Professor of Law at the University of Vermont Law School, discussed the connection between blockchain and the legal community. He first addressed how the law provides structure through legislation and then how blockchain provides promising benefits for the future application of law.

Goodenough argued that whether the law deals with blockchain through common law, legislation, or regulation will matter and will be important for the economy. He cited economist Paul Romer, winner of the 2018 Nobel Prize, who said:

> Economic growth is driven by the coevolution of two sets of ideas, technologies and rules. Governments can increase the rate of growth—in ways that benefit all citizens—by creating systems of rules that are both encouraging of and responsive to new technologies.[10]

Although some believe that the only governance needed on a blockchain is self-governance, that idea breaks down when legal proceedings begin. One recent lawsuit alleged the theft of 5,000 Bitcoins in 2012, or $32

[10] Paul Romer, *Bio*, LEIGH BUREAU (last visited Dec. 17, 2018), https://web.archive.org/web/20120606014844/http://www.leighbureau.com/speakers/promer/romer.pdf; *see also* Paul Romer, *Process, Responsibility, and Myron's Law*, in IN THE WAKE OF THE CRISIS: LEADING ECONOMISTS REASSESS ECONOMIC POLICY (eds. Olivier Blanchard, et al.), Cambridge, MA:MIT Press 2012.

million in value at the time of the suit.[11] Goodenough acknowledged that some states, like Vermont, have attempted legislative solutions, but the blockchain community could still benefit from additional legal clarity.

Many questions remain unanswered, such as what is the admissibility status of blockchain data in the courts; what is the legal status of smart contracts; and how will tokens and cryptocurrencies be regulated. Existing regulatory structures will be challenged by blockchain applications. For example, should tokens and cryptocurrencies be considered securities? If so, how does one comply with issuance regulations for an initial coin offering (ICO)? Once available, is a token a security or a commodity? What rules apply to the trading of such assets? Will the transfer of tokens and cryptocurrencies face roadblocks under anti-money laundering legislation?

Goodenough argued that there is also a need for new governance structures and that governments are beginning to recognize this need. The SEC recently announced the launch of the Strategic Hub for Innovation and Financial Technology (FinHub) to engage with the public and industry on new technological developments.[12] There are state legislative developments as well. Arizona has created a financial technology sandbox, which eases the regulatory burden on financial technology startups.[13] Wyoming and Vermont have also passed legislation regarding blockchain regulation. Goodenough noted possible future legislative and regulatory activity could include safe harbors for ICOs and trading, small purchaser exception, and nimble disclosure requirements, but also that blockchain will drive us to new regulatory formations we have not thought of yet.

As the legislatures become better at regulating the products of blockchain, the legal system will benefit from stability. Goodenough predicted that blockchain applications can lead to solutions for current privacy concerns, the creation of new property rights, the development of smart contracts, and commercialized arbitration. These solutions will likely be enabled by the legislature, not the courts. Courts will, however, play a key role in allowing change in this area by enforcing the law.

VI. Admissibility of Blockchain Evidence

Center Faculty Director Gary Marchant and Grant Autrey, a JD Candidate at the Sandra Day O’Connor College of Law, presented on the question of the admissibility of blockchain evidence in the courts. To properly admit evidence in court, the evidence must be relevant, reliable, and authenticated. Marchant and Autery focused on the latter two criteria because the relevance inquiry for blockchain evidence likely would be the same as for others types of evidence.

[11] Nathaniel Popper, *Bitcoin’s ‘First Felon’ Faces More Legal Trouble*, THE NEW YORK TIMES (Nov. 2, 2018), https://www.nytimes.com/2018/11/02/technology/bitcoin-charlie-shrem-winklevoss-twins.html.

[12] Press Release, U.S. Securities and Exchange Commission, *SEC Launches New Strategic Hub for Innovation and Financial Technology* (Oct. 19. 2018). https://www.sec.gov/news/press-release/2018-240

[13] Michael Del Castillo, *Breaking the Seal? Arizona Attorney General Opens Applications to First FinTech Sandbox*, FORBES (Aug. 3, 2018), https://www.forbes.com/sites/michaeldelcastillo/2018/08/03/breaking-the-seal-arizona-attorney-general-opens-applications-to-first-fintech-sandbox/#720cdae24616.

Marchant discussed how different jurisdictions are handling authentication of blockchain evidence. For example, Vermont recently passed legislation that provides for blockchain evidence to be self-authenticating:

> A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902, if it is accompanied by a written declaration . . . stating . . . :
>
> (A) the date and time the record entered the blockchain;
> (B) the date and time the record was received from the blockchain;
> (C) that the record was maintained in the blockchain as a regularly conducted activity; and
> (D) that the record was made by the regularly conducted activity as a regular practice.[14]

Similarly, Arizona passed legislation defining blockchain evidence as legal business documents, which fall under an authentication exception for admissibility.[15] At least one court in China, the Hangzhou Internet Court, ruled that documents authenticated with blockchain were admissible in a copyright infringement case:

> The court thinks it should maintain an open and neutral stance on using blockchain to analyze individual cases. We can't exclude it just because it's a complex technology. Nor can we lower the standard just because it is tamper-proof and traceable . . . In this case, the usage of a third-party blockchain platform that is reliable without conflict of interests provides the legal ground for proving the intellectual infringement.[16]

Government officials in the United Kingdom plan to conduct a pilot program for the storage of digital evidence on a blockchain.[17] Dr. Sadek Ferdous, Technology Policy Fellow and Research Associate at Imperial College, London, who attended the first meeting of the pilot program noted:

> [U]sing blockchain in evidence management creates a foolproof audit trail that tracks custody and can prevent evidence tampering. The audit trail forms the basis of the court's record of the creation, modification, and access to digital evidence by whatever entity handled it.[18]

Additionally, a recent amendment to Federal Rule of Evidence 902, which took effect in December 2017, permits self-authentication of digital evidence. These changes allow for the admissibility of

[14] 12 V.S.A. § 1913(b)(1).

[15] A.R.S. § 44-7061.

[16] Wolfie Zhao, *Blockchain Can Legally Authenticate Evidence, Chinese Judge Rules*, COINDESK (Jun. 28, 2018), https://www.coindesk.com/blockchain-can-legally-authenticate-evidence-chinese-judge-rules.

[17] Balaji Anbil, *How we're investigating Digital Ledger Technologies to secure digital evidence*, INSIDE HMCTS (Aug. 23, 2018), https://insidehmcts.blog.gov.uk/2018/08/23/how-were-investigating-digital-ledger-technologies-to-secure-digital-evidence/.

[18] Todd Gamo, *Digital Evidence Goes Blockchain in the UK*, IBINEX NEWS (Aug. 28, 2018), https://news.ibinex.com/2018/08/28/digital-evidence-goes-blockchain-in-the-uk/.

blockchain evidence if uncontested, but they do not answer the bigger problem of whether blockchain evidence is merely hearsay and therefore unreliable and not admissible.

Autrey focused on the issue of hearsay and why it may be a problem for the courts handling blockchain evidence. Hearsay—assertions of fact made out of court and being introduced to prove a matter at issue before the court—is generally inadmissible due to human error, such as erroneous memory, faulty perceptions, and insincerity, which can make such evidence too unreliable for use in court. While blockchain technology itself would not be considered hearsay evidence, any information stored on the blockchain likely would be. Such information is as susceptible to hearsay objections as any other piece of evidence.

While attempting to admit blockchain evidence would likely draw hearsay objections, it may also fit into well-established hearsay exceptions. Blockchain evidence may fall under the business records exception, so long as the information is kept on a blockchain as part of a regular business practice. Blockchain evidence may also be admissible under the 9th Circuit opinion in *U.S. v. Lizarraga-Tirado*.[19] Under that ruling, information produced through work done automatically by a computer is not an assertion and therefore cannot be considered hearsay.[20] Applying this decision to blockchain allows some information generated by the self-authenticating technology to be admissible and entirely sidestepping the issue of hearsay.

The main question for courts will be whether the evidence has sufficient probative value. Autrey said courts should evaluate evidence and determine admissibility, rather than letting the issue be addressed through legislation. Courts, on a case-by-case basis, are in the best position to decide the value of blockchain evidence. Additionally, the relevant technology is constantly and rapidly changing. By the time legislation regarding blockchain evidence makes its way through the legislative process, the technology may have changed enough to make the legislation obsolete or even a hindrance to the admission of such evidence.

VII. "Discovering" Blockchain Evidence

Antigone Peyton, Member at Protorae Law, presented on discovery of blockchain evidence. Peyton focused on discovery issues involving cryptocurrencies, such as Bitcoin, and the conversion of cryptocurrencies into traditional legal tender. This exchange of currencies has become a problem in a number of areas, including family law. For example, during a divorce one spouse may convert assets into cryptocurrency and hide them in a nearly untraceable account. Peyton warned against fixating on the blockchain rather than on the evidence itself.

Although the blockchain might be where the specific evidence can be found, the decentralized, anonymous, and secure nature of blockchain technology makes almost any attempt at direct discovery a fruitless endeavor. Instead of looking at the blockchain itself, attorneys need to look at either the specific cryptocurrency tokens being used or off-chain activity associated with a blockchain wallet. While blockchain technology allows individual users to remain anonymous, it also makes tracing tokens fairly easy. Targeted discovery is possible on both private and public blockchains. For private blockchains, where

[19] *U.S. v. Lizarraga-Tirado*, 789 F.3d 1107 (9th Cir. 2015).
[20] *See id.* at 1109.

users are identified, tracing the activities of a token allows one to easily track users and determine who to target for information. If the blockchain is public, where users are anonymous, tracing the activities of tokens is still useful for determining which accounts are relevant to an investigation and to narrow the scope of discovery.

Peyton said that the key to tracking down anonymous users is to look at off-chain activity that can be associated with an individual account. Users are still humans. They are likely to connect their anonymous blockchain account to another identifiable account, such as mobile apps, social media profiles, or cryptocurrency exchanges. An example of how this has been implemented in real life is a recent request by the IRS for information on users, including wallets and other identifiable information, from the cryptocurrency exchange Coinbase. Parties looking for information can, like the IRS, look for identifiable public entities where blockchain information goes in and out for various purposes. It is also important for discovering parties to understand how a blockchain is implemented and how the records are kept so that the tracing of users can lead to identification and discovery.

Finally, Peyton discussed some of the difficulties with discovering blockchain evidence. Sometimes, even if a party knows who owns a blockchain wallet with assets critical to a case, accessing the wallet can be a difficult task. Many blockchain users keep their blockchain wallet on offline devices, such as external hard drives or USB devices. If this is the case, it can be difficult to determine where the wallet physically resides or if the traced individual is the actual wallet holder without an experienced digital forensic expert available to determine if the wallet was used with the device traced to a user. The necessity for an expert in such a case can create multiple problems, not just because of the increased cost and difficulty of the discovery, but also because it can be difficult to have blockchain experts explain the information in a way a jury can understand. According to Peyton, courts struggle with blockchain experts because expert testimony often boils down to “you’ll just have to trust me that I know how this works.”

While discovering blockchain evidence may seem intimidating, if not impossible, by changing the focus of discovery investigation away from the blockchain itself, the process becomes a bit easier. Lawyers and discovery professionals need to stop looking at ways to attack the blockchain for information and instead should try to work with the blockchain. Tracing transactions on a blockchain is a built-in benefit of the technology, and with the growing use of cryptocurrencies so too grows the number of institutions with discoverable information. By using the tools currently at our disposable, finding evidence on a blockchain can be accomplished and traditional modes of discovery still apply.