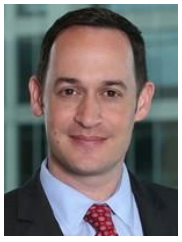
3 Lessons From A Crypto Mock Trial

By **Justin Steffen, Andrew Hinkes, Lisa Braganca, Christopher Veatch, Kashan Pathan and Jimmie Zhang** (February 22, 2019)

Justin Steffen



Andrew Hinkes

Lisa Braganca

Christopher Veatch

Kashan Pathan

Jimmie Zhang

We had each seen articles that wondered aloud whether blockchain ledger entries were admissible evidence in a court proceeding. With over 65 years of litigation experience combined, we too could envision the hearsay and authentication objections attorneys would inevitably assert when confronted by the adverse party's attempt to admit crypto evidence. Rather than opine, we sought to take action. As Einstein quipped, "the only source of knowledge is experience."

So, we hatched a plan to test whether litigators could actually get distributed ledger entries into evidence under the existing Federal Rules of Evidence. We collaborated to make a realistic fact pattern, elicited the help of a few carefully-curated witnesses, and instructed them to use their wits and act like real witnesses. Most importantly, we found a judge willing to help us on our journey of discovery. On Dec. 6, 2018, at Loyola Law School (Chicago), in front of Judge John Robert Blakey of the Northern District of Illinois and a packed house of technologists, lawyers and students, we put ourselves to the task, learning more than we had anticipated in the process.

First, we created a problem. Attorneys live for facts. Depending on who you ask, "facts" are not necessarily the truth; a lawyer will tell you facts are what you can prove at trial. If you cannot prove it, it may as well have never happened. Attorneys also, perhaps unsurprisingly, love to argue. So, we needed to develop a problem that would yield nuanced arguments and that would allow the attorneys and the audience to explore the issues and challenges presented by distributed ledger entries. We also sought to create a fact pattern that was as realistic as possible, relying on the types of evidence and witnesses that would be available in a real-life lawsuit. We settled on the following facts:

> A prominent tech investor hired a hit man to murder his estranged wife. The husband paid the hit man with cryptocurrency. The transaction was made in a peer-to-peer payment recorded on the cryptocurrency's blockchain. The prosecution was to establish that the payment occurred by introducing an exhibit — a printout of what was claimed to be the transaction details from a fictional blockchain explorer service's website. To aid in this task, the prosecution had three witnesses available to it: (1) a core developer who would attempt to testify to how the cryptocurrency blockchain functioned, and what was represented on the exhibit; (2) a representative from the blockchain explorer service who could testify to how the exhibit was created; and (3) a representative from a blockchain forensics firm who could try to tie the public key addresses to the husband and hit man.

Next, we assigned roles. Drawing on their years representing the government, Chris Veatch and Lisa Braganca morphed into the prosecution. Andrew Hinkes and Justin Steffen assumed the mantle of the defense. Kashan Pathan and Jimmie Zhang stepped into the roles of the blockchain explorer company witness and the developer witness, respectively. And, for the sake of time, the parties stipulated that the third witness — a witness from a fictional blockchain forensics company — would have testified that the public keys involved in the relevant transaction were, at one point, each associated with the husband and hit man, respectively.

Then, the teams prepared. In all ways, this exercise mimicked an actual federal trial. We briefed Judge Blakey, prepared the witnesses, drafted

examination outlines, and secured demonstrative exhibits. The parties agreed that the Federal Rules of Evidence would govern, and researched the rules and recent case law supporting or precluding the admission of various other forms of digital evidence. Witnesses were prepared to testify for multiple days. In all ways, we treated this exercise as if it were real.

Finally, we performed. Veatch and Braganca carefully put on their case through multiple witnesses. Hinkes and Steffen pressed every objection they could muster — relevance and unfair prejudice (FRE 401, 403), failure to authenticate (FRE 901), the best evidence rule (FRE 1002), hearsay (FRE 802), and even a Crawford objection. Veatch and Braganca countered, drawing on hearsay exceptions and a new rule created to help litigants self-authenticate electronically generated records (FRE 902(13)). The parties argued, and Judge Blakey "ruled."[1]

1. If Done Correctly, Pseudo-Anonymous Ledger Entries Are Admissible Into Evidence

The Rules of Evidence are sufficient. New rules, like Vermont's evidentiary statute, are not necessarily required. Hearsay objections can be overcome, foundation can be properly laid, and the right witnesses can authenticate transaction records. In ruling that the exhibit (the block explorer transaction history) could come into evidence at trial, Judge Blakey succinctly addressed each of the parties' arguments.

The defense, for example, argued that the exhibit was not relevant and was unfairly prejudicial because a document reflecting a transaction between two public keys does not definitively establish that a particular person or set of persons entered into a transaction. The defense argued that, without evidence of those particular persons having actually used the private keys, the prior association of the public key addresses with those persons was irrelevant, misleading and potentially confusing.

The judge, agreeing with the prosecution's argument, countered that the forensic expert's evidence that tied those public key addresses to the defendants was sufficient to overcome the defense's relevance objection. Judge Blakey reasoned, moreover, that although the exhibit was prejudicial, it was a key piece of circumstantial evidence and not "unfairly prejudicial." Indeed, Judge Blakey noted that "if it wasn't prejudicial, it wouldn't be relevant or be a government exhibit."

The defense also argued that the exhibit was inadmissible hearsay that could not be authenticated because no one person or entity controlled the blockchain. Again, agreeing with the prosecution's argument, Judge Blakey likened the record to a verbal or "mechanical act" akin to the display of time on a clock, rather than an out-of-court statement. The judge, moreover, noted that the Rules of Evidence require authentication only from a person with knowledge and that the witnesses put on by the prosecution not only had knowledge of how the blockchain worked but also of how the transaction was recorded on the block explorer service.

In this case, the prosecution took the steps essential to overcome the myriad evidentiary hurdles, and Judge Blakey admitted the exhibit. It is important to note, however, were this a real trial, most if not all of the defense's admissibility objections could have been repackaged and presented as closing arguments, minimizing the weight the jury should afford such evidence.

2. Preparation Is a Must

Distributed ledgers and cryptocurrencies may seem relatively straightforward to crypto enthusiasts, but to most casual onlookers, and particularly to juries and busy judges, crypto concepts may not be second nature. To help the uninitiated understand blockchain-based evidence, proponents must lay the proper foundation and clearly convey highly technical mathematical concepts (e.g., the reliability and security of SHA-256 encryption).

As with other highly complicated subject matters, attorneys tasked with introducing crypto evidence must be prepared to argue and to clearly communicate technical concepts in

layman's terms without distorting their accuracy. Attorneys will need to dedicate the appropriate time necessary to help the finder of fact understand the nuances and complexities of distributed ledger technologies.

Attorneys, moreover, will need to select their analogies carefully, and prepare to defend and distinguish those examples from the unfavorable comparisons their opponents will inevitably draw.

For example, those seeking to introduce a blockchain ledger into evidence may argue the blockchain ledger is no different from a billing invoice prepared by a cellphone provider illustrating monthly call records. It involves no human intervention or interpretation; it is simply the record of a transaction. Those opposing the evidence may attack that analogy, as cellphone records cannot be changed simply because 51 percent of the cellphone company's customers agree to do so.

The typical back-and-forth of litigation may ultimately confuse a jury or judge if counsel is not prepared to delve deeply into the inner workings of crypto and blockchain. The knowledge required to effectively litigate crypto claims is significant. Un- or under-prepared attorneys run the risk of being twisted into knots by their more adept adversaries.

3. Discovery Is Key

Trials are the culmination of many months or even years of preparation. Attorneys should begin planning how to get blockchain-related transactions into evidence as early as possible. Specifically, attorneys will need to understand the technology and to identify what third-party service provider witnesses are necessary to surmount the evidentiary hurdles. If counsel fails to comprehend the nuances of blockchain technology, they may not be able to identify, request and obtain the critical evidence in the case. Likewise, they may fail to comprehend which witnesses they will need to call at trial to overcome the evidentiary objections or to concisely explain the technical concepts involved.

Litigation truly is a marathon, not a sprint. And while a marathon cannot be won in the first few miles, it may be lost. As blockchain and crypto are poised to permeate the litigation landscape, regardless of practice area, counsel need to take the time to learn as much as they can about blockchain well in advance of the trial or even discovery.

Justin Steffen is a partner at Ice Miller LLP and a fintech law professor at Loyola Law School (Chicago).

Andrew Hinkes is the general counsel of Athena Blockchain and an adjunct professor at NYU School of Law and NYU Stern School of Business.

Lisa Braganca is the founder of Braganca Law LLC and the former branch chief for the Chicago office of the U.S. Securities and Exchange Commission's Division of Enforcement.

Christopher Veatch is a partner at Perkins Coie LLP and former chief of the National Security and Cybercrimes Section with the U.S. Attorney's Office for the Northern District of Illinois.

Kashan Pathan is an assistant U.S. attorney and former associate at Jenner & Block LLP.

Jimmie Zhang is a legal and policy adviser to the Illinois Commerce Commission and a former adviser to Athena Bitcoin, Finalyze, and other technology companies.

[1] Judge Blakey's participation in this event was purely for educational purposes. His rulings and comments should not be construed as precedential, an advisory opinion, or indicative in any way of how he may view evidence and arguments in actual (as opposed to moot court) proceedings.