ILLINOIS STATE BAR ASSOCIATION

NOVEMBER 2019 VOL 66 NO. 3

Trial Briefs

The newsletter of the Illinois State Bar Association's Section on Civil Practice & Procedure

Blockchain as Evidence

BY GEORGE "GEO" BELLAS

Despite the hoopla, most attorneys know absolutely nothing about blockchain. Bitcoin—a virtual currency—is the first and most popular application of blockchain technology, but blockchain has much broader applications. Over the next several years lawyers can expect to be dealing with blockchain issues with increasing frequency. Blockchain will be an issue in divorces, business acquisitions, estate planning, real estate, employment, personal injury, and practically every aspect of business. This technology will create new opportunities for business owners and lawyers. And it will create issues during trial as courts struggle to understand it and deal with it.

What Is Blockchain?

The concept of a blockchain was first conceived in 2008 by someone named Satoshi Nakamoto, which may be pseudonym for someone or a group of people, who introduced a white paper[1] describing the open-source block chain technology that underlies the basis for the cryptocurrency known as Bitcoin.

Blockchain is a totally disruptive technology and is now being used in many industries to create a shared, immutable record of any asset to create a tamper proof record of the asset or record. This avoids the necessity of relying on an old-fashioned record or database. It makes the record virtually impossible to tamper with. Blockchain actually makes a record more trustworthy because it builds on every other transaction. Any changes or corruption is readily apparent.

Basically, blockchain is a method of adding new data into a system. The data is added to the block in a blockchain by connecting it with other blocks in chronological others creating a chain of blocks linked together. Data can only be added in the blockchain with time-sequential order, which makes it very difficult to modify and thereby making it very secure. The data is not located in one location—it has no central authority or master. Rather, the data is located in aggregates (or "blocks") that are time-stamped and form a immutable chain of sequenced data—which is where the name "blockchain" is derived. This distributed network provides security and continuity since any attempt to change or hack the system will show the altered version is inconsistent with the copies at the other points in the chain. Hospitals are now using it to store patient records in a highly protected system while allowing sharing between hospitals, providers, and insurance companies. Blockchain has also become the centerpiece of a radical change in financial technologies known as "FinTech."

Cryptocurrency Is an Application of Blockchain Technology

Blockchain is the underlying technology that forms the basis of digital currencies or "cryptocurrency." Cryptocurrency is nothing more than a digital asset created independently from any government or bank.

In the traditional exchange of money, the money is transferred thru an intermediary—usually a bank—which takes a commission on the transaction.

On the other hand, in cryptocurrency technology the intermediary is a blockchain which is a collective group of systems that verify the transaction. It is faster, more secure and easily more traceable than a bank transaction. It begins when you decide to accept payment for services or a product by Bitcoin or another form of cryptocurrency.

Bitcoin is only one of several forms of digital currencies which includes Litecoin, Ethereum, and others. The technology underlying blockchain creates a type of digital ledger that is stored in a wide-ranging network. The data is stored on multiple computers at the same time. When data is added to the chain, it adds to the existing block of data and creates a chain of data.

Illinois Steps Up to the Block

Some states have already adopted legislation that promotes the development and use of blockchain. Illinois continues to be a leader in technology-related legislation. Under the Illinois Blockchain Technology Act,"blockchain" is defined as "an electronic record created by the use of a decentralized method by multiple parties to verify and

store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information." Among other things, the Act specifies permitted uses of blockchain technology in transactions and proceedings, such as in smart contracts, electronic records and signatures, and provides several limitations, including a provision stipulating that if a law requires a contract or record to be in writing, the legal enforceability may be denied if the blockchain transaction cannot later be accurately reproduced for all parties. The Illinois Blockchain Technology Act takes effect in January 2020.

Blockchain will serve to authenticate records and will form the basis of "smart contracts" that will protect the parties and insure performance. There are many uses of blockchain technology that are far beyond the intended scope of this article and there are multiple legal implications of the use of the technology.

Blockchain on Trial – A New Evidentiary Issue

Lawyers will be facing the problem of introducing blockchain data into evidence at trial. Sounds daunting, but it is really not that complicated.

Essentially, a blockchain is a piece of digital data. Because of it is inherent trustworthiness, it should be relatively easy to establish the authenticity of the digital evidence.

The Federal Rules of Evidence ("FRE") has as a basic tenet the requirement for the best evidence to be used at trial. FRE 1002 is referred to as the best evidence rule and requires the production of the original document in court when relevant. FRE 1002 states: "An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise."

Sounds simple, but in the digital age this could be difficult, particularly when the hearsay rule (and exceptions) rears its confusing head. Ener the "Lizarraga-Tirado test" which is based on the case of *U.S. v. Lizarraga-Tirado*, 789 F.3d 1107 (9th Cir., 2015). In this case the court was confronted with the issue of authenticating the thumbtack position on a Google Earth screenshot which was used to determine the location of an arrest. The court admitted the screenshot because the screenshot – the satellite image of the area – is not hearsay. It is merely a photograph of the earth taken by a satellite and makes no assertion. It is, therefore, not hearsay.

The thumbtack position on the image is a different issue. Since the thumbtack is automatically generated by the computer program, it is not a statement as defined by the hearsay rule and the placement of the thumbtack requires some authentication—an objection that was not raised by the defendant. Basic evidence law requires a proponent of the evidence show the authenticity of the proposed evidence for admissibility purposes.

> Authentication requires the proponent of evidence to show that the evidence "is what the proponent claims it is." Fed.R.Evid. 901(a). A proponent must show that a machine is reliable and correctly calibrated, and that the data put into the machine (here, the GPS coordinates) is accurate. See Washington, 498 F.3d at 231. A specific subsection of the authentication rule allows for authentication of "a process or system" with evidence "describing [the] process or system and showing that it produces an accurate result." Fed.R.Evid. 901(b)(9); see also United States v. Espinal–Almeida, 699 F.3d 588, 612 (1st Cir.2012) (evaluating whether "marked-up maps generated by Google Earth" were properly authenticated). So when faced with an authentication objection, the proponent of Google Earth–generated evidence would have to establish Google Earth's reliability and accuracy. That burden could be met, for example, with testimony from a Google Earth programmer or a witness who frequently works with and relies on the program. See Charles Alan Wright & Victor James Gold, Federal Practice & Procedure § 7114 (2000). It could also be met through judicial notice of the program's reliability, as the Advisory Committee Notes specifically contemplate. See *id*.; Fed.R.Evid. 901 n.9. United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir., 2015).[2]

Authentication of Blockchain Data

The problem with authentication in Illinois should now be solved by the adoption of IRE 902(12) and 902(13) in 2018.[3] New IRE 902(12) is aimed at digital copies, making the following self-authenticating:

> (12) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

The key to the rule is that it requires some technological expertise to certify the digital record. But this is easy to accomplish if you take advantage of the provisions of IRE 902(11) which allows for authentication by affidavit and proper notice.

IRE 902(12) simply allows use of a certification to authenticate evidence generated by an electronic process or system (e.g., the contents of a website, data generated by an app, electronic entry/exit records of a security system). Rule 902(12) authorizes a certification to authenticate a digital copy of data taken from a device or system (e.g., a mobile phone, a hard drive).

This can be accomplished by using the "hash value" of the record. According to the

Sedona Conference Glossary: E-Discovery & Digital Information Management (4th Edition) the "hash code" of a record is defined as:

> Hash Coding: A mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified. Common hash algorithms include MD5 and SHA. See Data Verification, Digital Fingerprint, File Level Binary Comparison.

Essentially, the hash value or hash code is used to identify, verify and authenticate file data. Hash functions have many uses in the digital world, the most important for the blockchain is in validating the integrity of a file. This simply means that a technician will certify that the data copied is verified to be identical to the codes in the original file by comparing the hash codes of the original to the copy.

This certification can be accomplished by an affidavit of the technician who extracts the data. The extraction is then saved and an expert or technician certified that the data in the copy is identical to the original. The certification is filed with a digital copy and notice of the intent to use the record must be provided to the other parties in accord with IRE 902(11).

A certification under IRE 902(11) can also be combined with the IRE 902(12) certification to establish that the information was maintained in the ordinary course of business and the process used to generate the record is itself authentic. The Illinois Blockchain Technology Act permits a blockchain to be used in a proceeding provided it can be properly authenticated. (See Section 10 of the Act)

Thus, a digital record from a blockchain is self-authenticating and admissible when introduced by a written declaration (affidavit) by a qualified person under Rule 902(11). This rule is not well known to Illinois practitioners, but it should be an essential tool in the lawyer's toolbox.

Conclusion

Some states are moving ahead and advancing specific rules to authenticate blockchain data. For example, Vermont passed H.868 (Act 157) stating that: "A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence." Illinois has not yet done so.

Illinois lawyers can now practice in a blockchain-friendly environment and advance uses of this technology in smart contracts and chain of ownership. We can encourage blockchain research and innovation in all industries in the state. However, the technology will require Illinois practitioners to keep abreast of the advances in technology and learn how to use it at trial.■

George "Geo" Bellas is a 10-year member of the ISBA Civil Practice and Procedure Committee, a member of the 7th Circuit Council on eDiscovery & Digital Information, and a frequent lecturer on the use of technology at trial.

1. https://bitcoin.org/bitcoin.pdf, which details methods of using a peer-to-peer network to generate what was described as «a system for electronic transactions without relying on trust."
2. 789 F.3d at 1110.
3. The Federal Rule of Evidence equivalent of IRE 902(1) is FRE 902(14) adopted in 2017.

Reprinted with permission of the Illinois State Bar Association
Vol. 66 No. 3
www.isba.org