BLOCKCHAIN AS EVIDENCE: HOW WILL IT GET INTO COURT?

Alex Ashrafi

BLOCKCHAIN: AN OVERVIEW

Since Satoshi Nakomoto's paper sparked the concept of blockchain technology, the world has opened its imagination to the countless applications of blockchain.[1] Although cryptocurrencies like Bitcoin initially used blockchain to revolutionize money, this technology has also been used for many other purposes, including finance, real estate, and compliance.[2] One of blockchain's biggest strengths is its supposed immutability. Due to its decentralized design and hashing algorithm,[3] it is very difficult (though not impossible) to hack the blockchain and falsify its records. A person that is legally-minded might immediately realize that a technology which enhances authenticity has a glaring application to a particular area of law—evidence.

As more important information is kept within records in a blockchain, it will undoubtedly prove to be valuable for litigating certain legal issues. With disputes concerning blockchain (such as Bitcoin) going to court, it is inevitable that blockchain ledgers will make their way into courts as evidence. The question becomes whether courts will recognize the unique nature of blockchain that authenticates the information held within its distributed ledger. Other nations' courts have been more active in adapting to blockchain. China's Supreme People's Court has already passed rules that recognize data stored within blockchain as authenticated evidence.[4] The U.K. is experimenting with a pilot program that uses

---

[1] Sataoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (Nov. 1, 2008), https://bitcoin.org/bitcoin.pdf.

[2] Nolan Bauerle, *What Are the Application and Use Cases of Blockchain?*, COINDESK, https://www.coindesk.com/information/applications-use-cases-blockchains (last visited May 23, 2019); *see also* Brooke Roberts-Islam, *World's First Digital Only Blockchain Clothing Sells For $9,500*, FORBES (May 19, 2019, 2:12 PM), https://www.forbes.com/sites/brookerobertsislam/2019/05/14/worlds-first-digital-only-blockchain-clothing-sells-for-9500/#462ba982179c.

[3] A hashing algorithm takes a string (a phrase or number, for example) and converts it into a unique key that can be used to access the original data. For a layman's explanation of hashing, see Liberty York, *What is Hashing?*, MEDIUM (Feb. 22, 2018), https://medium.com/tech-tales/what-is-hashing-6edba0ebfa67.

[4] Wolfie Zhao, *China's Supreme Court Recognizes Blockchain Evidence as Legally Binding*, COINDESK (Sept. 7, 2018, 4:00 AM), https://www.coindesk.com/chinas-supreme-court-recognizes-blockchain-evidence-as-legally-binding.

blockchain to secure evidence that parties introduce in courts.[5] The United States, meanwhile, has not formally recognized blockchain's utility with evidence just yet. However, examining recent amendments to the Federal Rules of Evidence, state laws, and other analyses of electronic evidence may shed some light on how courts might similarly recognize blockchain's use in evidence authentication.

At its most basic level, blockchain can be described purely from its name—a chain of "blocks" storing information. Each block contains data, a unique hash code to identify that data,[6] and the hash code of the previous block in the chain that the current block points to. When the data within a block is changed, the hash of that block changes as well. This feature increases the security of blockchain, as a hacker would have to recalculate the hashes of all the blocks indirectly connected to the block the hacker tampered with, which would require a great amount of computing power.

Additionally, blockchain is decentralized and distributed across a network of computers. This means that any change to the chain is broadcast to all the network participants, each of whom holds an identical copy of the blocks contained in the chain, usually referred to as the ledger. For a node[7] to add a block (containing a record of a transaction or other data) to the blockchain, it must use a method to verify the transaction. A very common method is showing proof-of-work by solving a complicated math problem requiring significant computing power. A participant who solves these math problems to add blocks and validate transactions is called a "miner." The other participants' computers on the network will verify the miner's proof-of-work, after which the new block will be added. Miners are incentivized to participate in this process by receiving a fee—usually a crypto coin—for each transaction they validate. This verification, computing power requirement, and decentralized design all ensure trust in the data held within a blockchain.[8]

---

[5] David Hundeyin, *UK Government Pilots Storage of Digital Evidence on a Blockchain*, CCN (Aug. 26, 2018, 11:42 AM), https://www.ccn.com/uk-government-pilots-storage-of-digital-evidence-on-a-blockchain.

[6] A hash code is a unique key that "points" to a specific object, in this case a block. *See supra* note 3 and accompanying text.

[7] A node is a device participating in the network. *See Let's Talk About Bitcoin Nodes*, HACKERNOON (Nov. 10, 2017), https://hackernoon.com/lets-talk-about-bitcoin-nodes-e9502193198c.

[8] *See, e.g.*, Sean Caputo, *3 Ways to Gain Audience Trust in Blockchain*, BUSINESS.COM (Aug. 13, 2019), https://www.business.com/articles/3-ways-to-gain-audience-trust-in-blockchain/.

One might therefore say that blockchain is, technically speaking, self-authenticating, but would evidence law recognize it as such?

IS BLOCKCHAIN SELF-AUTHENTICATING EVIDENCE?

Rule 902 of the Federal Rules of Evidence lists the types of self-authenticating evidence which "require no extrinsic evidence of authenticity in order to be admitted."[9] Most types of evidence listed in Rule 902, like certified public documents or newspapers, do not need any additional evidence to authenticate. A few others, namely records of regularly conducted activity, require the party introducing the evidence to certify its authenticity—which can be done prior to trial—and allow the opposing party to challenge the authenticity before trial.[10]

In December 2017, an amendment to Rule 902 added new types of self-authenticating evidence to this list under subsections 902(13) and (14). Now, certain data that is electronically-generated[11] or copied from an electronic device or file[12] can be admitted on their own without having to be authenticated by a live witness under Rule 901.[13] However, like records of regularly conducted activity, electronically-generated data is not automatically authenticated.[14] The introducing party still needs to provide some extrinsic evidence along with the electronic evidence and give the opposing party a chance to challenge the authenticity.[15] Usually, this extrinsic evidence would be in the form of an affidavit from an expert explaining how the electronic system works and why its data is reliable.[16] Still, adding electronically-generated evidence to Rule 902 simplifies the process of admitting electronic evidence by allowing parties to settle any authenticity disputes before trial without live witnesses.[17] Regarding blockchain, the question is whether data from blockchain counts as self-authenticating evidence under Rule 902.

---

[9] FED. R. EVID. 902(13)–(14).
[10] *Id.* 902(11).
[11] *Id.* 902(13).
[12] *Id.* 902(14).
[13] Carl A. Aveni, *New Federal Evidence Rule Changes Reflect Modern World*, ABA (Apr. 23, 2018), https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/new-federal-evidence-rule-changes-reflect-modern-world.
[14] *See id.*
[15] *See id.*
[16] *See* Paul W. Grimm & Kevin F. Brady, *Recent Changes to Federal Rules of Evidence: Will They Make It Easier to Authenticate ESI?*, 19 SEDONA CONF. J. 707, 718 (2018).
[17] *Id.* at 715.

THE PROCESS IN PRACTICE: VERMONT'S NEW EVIDENCE RULES

Vermont addressed the question posited above by passing a law stating that "a digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902."[18] Mirroring the Federal Rule 902 requirement to provide an affidavit verifying the authenticity of electronic data, the Vermont statute imposes additional requirements to demonstrate the record's authenticity. Specifically, it requires the blockchain record be accompanied by a written statement under oath from a qualified person that states: the date and time the record was entered on and subsequently received from the blockchain; that the blockchain maintained the record as a regularly conducted activity; and that the record's making was a regular practice.[19] In other words, a live witness is no longer required to authenticate a record in a blockchain as long as the party producing it can satisfy the requirements to verify it.

Following the Vermont Statute, Vermont Rule of Evidence 902 was amended in early 2019 to mirror the language in the statute by adding a new section in the rule for blockchain records.[20] The advisory committee's notes state that records admitted under the blockchain provision would have to fulfill very similar conditions to records admitted under the regularly conducted activity provision, and in many cases would be admissible under that section.[21] The amendments were made in case there is doubt whether certain records maintained in the blockchain satisfy every piece of language in the existing exception.[22] Lawyers wanting to introduce blockchain records as self-authenticating evidence can now do so under this specific section.

Vermont also appears to address any hearsay issues that may arise from the blockchain record. By requiring the record to be part of a regularly conducted activity and a qualified person to certify the record, evidence that satisfies Vermont's authentication requirement should also qualify as a "business record" exception to hearsay.[23] However, there are cases in which blockchain data still might not qualify for the exception. Although the blockchain might have produced the given evidence as regularly conducted activity, a court might find that the actual transaction within the record is not

[18] VT. STAT. ANN. tit. 12, § 1913(b)(1).
[19] *Id.*
[20] Vt. R. Evid. 902(13).
[21] Vt. R. Evid. 902, advisory committee's notes.
[22] *Id.*
[23] *See* FED. R. EVID. 803(6).

regularly conducted activity.[24] Then again, the blockchain evidence might not even be hearsay if it is, for example, part of a smart contract. In that case, the "statement" in the record would hold independent legal significance just as traditional contracts would.[25]

Moreover, the Vermont statute and the amendment to Vermont Rule 902 do not require that the record be made by someone with knowledge, as the regularly conducted activity provision (and hearsay exception) requires.[26] Unlike a regularly conducted activity recorded in a document by a person, the record in a blockchain is technically recorded by the miner that adds the block. The miners recording transactions in blocks inherently have knowledge of the transaction they are recording, though not in the conventional form contemplated by these evidentiary rules. Thus, language in the statute or rule requiring the record be made by someone with knowledge seems ill-suited and unnecessary in the context of blockchain.

Vermont's inclusion of blockchain in its evidence rules aligns with other policy changes in the state that encourage blockchain use. Hoping to attract new companies that use blockchain, the state recently passed another law that creates the "blockchain-based limited liability companies" business entity.[27] Additionally, municipalities in Vermont have begun using blockchain for real estate transactions, particularly to record property titles.[28] Given that legal disputes are bound to arise involving blockchain business entities and property data stored in

---

[24] *See* FED. R. EVID. 803, advisory committee's notes (using the example of a police officer recording information from a bystander in a report. Although the making of the report was a regularly conducted activity, the bystander did not act in a regular course of business in giving the information). Similarly, a blockchain might act in a regular course of business in recording information (like the officer), but the party giving the blockchain the information might not (like the bystander). *See* Neil Gray & Maxwell J. Eichenberger, *Blockchain: Immutable Ledger, But Admissible Evidence?*, N.Y.L.J. (Dec. 14, 2018), https://www.law.com/newyorklawjournal/2018/12/14/blockchain-immutable-ledger-but-admissible-evidence (citing the same example from the advisory committee's notes).

[25] *See* Gray & Eichenberger, *supra* note 24.

[26] *See* Vt. R. Evid. 902(11) (requiring that the record was made by "a person with knowledge of those matters").

[27] Xander Landen, *Vermont bullish on blockchain as new law takes effect*, VTDIGGER (Aug. 28, 2018), https://vtdigger.org/2018/08/28/vermont-bullish-blockchain-new-law-takes-effect.

[28] *See* VERMONT LEGISLATIVE REPORT ON BLOCKCHAINS FOR PUBLIC RECORDKEEPING & FOR RECORDING LAND RECORDS (Jan. 15, 2019) (on file with author).

blockchains, it makes sense that Vermont would update its evidence rules to accommodate blockchain.

COMPARING VERMONT TO OTHER STATES' APPROACHES

Although Vermont is currently the only jurisdiction to directly include a section for blockchain in its self-authenticating evidence rule, other states have made similar modifications to various laws to clear up any questions about the admissibility of records secured by blockchain. In August 2018, Ohio modified its definitions of "electronic record" and "electronic signature" in its Uniform Electronic Transactions Act to include records and signatures secured through blockchain.[29] Arizona made similar changes to its electronic transaction law in April 2018, while also adding a provision that upholds the legal effect of smart contracts.[30] However, most jurisdictions have not created laws or amended their laws to account for blockchain.

The practical reality of how blockchain transactions are verified, and the clear intent of the Vermont rule drafters to model the blockchain-specific rules of evidence after business records exceptions, begs the question whether blockchain evidence, evaluated by traditional rules of evidence will experience greater difficulties with admissibility. This is especially so in light of the notable decision to remove the requirement that the evidence be authenticated, certified, or otherwise submitted by "someone with knowledge."[31] It is possible that courts will take a broader view of "knowledge" to include the complex nature of blockchain mining and trust, but others may find that no party—including the miner—has sufficient knowledge of the *nature* of the specific transaction to speak to either the authenticity of the evidence or its trustworthiness under the hearsay rules.

However, as a recent mock trial suggests, it might not even be necessary to make amendments to evidence, as Vermont has done. [32] Attorneys recently conducted a mock trial specifically to see whether blockchain evidence could be admitted under the Federal Rules of Evidence.[33] They found that records from a blockchain could be admitted under the existing rules without additional rules like Vermont's. That said, attorneys seeking to introduce this

---

[29] OHIO REV. CODE ANN. § 1306.01 (West 2019).
[30] ARIZ. REV. STAT. ANN. § 44-7061 (2019).
[31] *See supra* text accompanying notes 17–23.
[32] Justin Steffan et al., *3 Lessons from a Crypto Mock Trial*, LAW360 (Feb. 22, 2019), https://www.law360.com/articles/1131844/3-lessons-from-a-crypto-mock-trial.
[33] *Id.*

evidence must be prepared to explain the workings of blockchain technology to the finder of fact with appropriate witnesses. Vermont's rules expedite this process by allowing attorneys to introduce blockchain evidence before trial, supported by affidavits, but it is certainly possible to admit blockchain-based evidence without such additional accommodations, according to the results of the mock trial.

Two caveats are important to highlight. First, the results are limited to a single *mock* trial, with no precedential value, raising questions of replicability and external validity.[34] Second, the ability to locate "appropriate witnesses" in a pseudonymous context such as blockchain, and the time, attention, and expertise—from both witnesses and the presenting attorneys—to explain how blockchain works may present considerable barriers to many clients that cannot afford blockchain experts. While the mock trial encouragingly demonstrated that it may be possible under the right conditions, it is no guarantee that the path will be clear for attorneys seeking to present blockchain evidence in court.

Just as it has been with other forms of technology, as more businesses and local governments implement blockchain in a variety of ways throughout U.S. jurisdictions, adjustments to the respective evidence rules will be sure to follow. It will be particularly interesting to see whether states with larger economies or greater influence over securities—such as California, New York, and Delaware—will amend their evidence rules to accommodate blockchain, as data secured by blockchain in those states will likely enter courts faster and in a higher volume.

USING BLOCKCHAIN TO AUTHENTICATE EVIDENCE

Perhaps a more revolutionary application of blockchain in the courts comes not in the form of admitting data stored within blockchains as evidence, but in using blockchain to authenticate evidence introduced in court. While the former merely recognizes blockchain, without requiring live expert testimony to explain the technology each time attorneys try to introduce it, the latter adopts blockchain as a tool to store digital evidence.

Electronic evidence can reduce costs and time in courts by making evidence more easily-accessible, assuming such electronic evidence is compatible with the technology of courts (which is not always the case).[35] The downside of electronic evidence is that it can

---

[34] *Cf. id.*

[35] *See, e.g.*, Sean E. Goodison et al., *Digital Evidence and the U.S. Criminal Justice System*, PRIORITY CRIM. JUST. NEEDS INITIATIVE (2015), https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.

be easily modified or fabricated.[36] Blockchain is a potential solution to this security concern—particularly permissioned blockchains, in which participants need consent before accessing or becoming part of the network. The U.K., for example, is currently testing a program that will store digital evidence on a blockchain.[37] Likewise, the Dubai International Financial Center (DIFC), a Dubai-based international court, announced in July 2018 that it is developing a "blockchain-based legal platform" that will put court data onto blockchain, allowing parties and other institutions to exchange and verify authentic information instantaneously.[38] Blockchain can also create a secured audit trail to track custody of evidence. This feature would ensure that evidence admitted is protected throughout the proceeding, certifying the evidence's authenticity. There will be a guarantee that evidence accessed at any point in court proceedings will be identical to the original evidence input into the electronic system.[39]

While a potential asset for courts as evidence preservation and recordkeeping, the implementation of such systems in U.S. courts is likely a long way off. As a new technology, blockchain would need to overcome some—arguably warranted—skepticism about its legitimacy, cybersecurity, and the overall inertia against change in legal community. The legal profession, and especially courts, have been slower to adopt or make use of courtroom or courthouse technology, let alone cutting edge emerging technologies.[40] Amidst myriad financial and other challenges faced by today's federal, state, and local courts,[41] testing out what are still

---

[36] Paul Sachs, *The Law & Courts: The Case for Blockchain*, LAW. MONTHLY (Aug. 13, 2018), https://www.lawyer-monthly.com/2018/08/the-law-courts-the-case-for-blockchain.

[37] *See* Hundeyin, *supra* note 5.

[38] Wolfie Zhao, *Dubai Plans to "Disrupt" Its Own Legal System with Blockchain*, COINDESK (July 30, 2018, 9:00 AM), https://www.coindesk.com/dubai-plans-to-disrupt-its-own-legal-system-with-blockchain. *See also* Press Release, DIFC Courts, DIFC Courts and Smart Dubai Launch Joint Taskforce for World's First Court of the Blockchain (Jul. 30, 2018), https://www.difccourts.ae/2018/07/30/difc-courts-and-smart-dubai-launch-joint-taskforce-for-worlds-first-court-of-the-blockchain/.

[39] *See* Sachs, *supra* note 36.

[40] *See, e.g.*, Jeff Charles, *The Legal Industry is Finally Fixing Its Technology Problem*, SMALL BUS. TRENDS (Jan. 11, 2019), https://smallbiztrends.com/2017/02/legal-technology.html; Mark A. Cohen, *Lawyers and Technology: Frenemies or Collaborators?*, FORBES (Jan. 15, 2018, 5:56 AM), https://www.forbes.com/sites/markcohen1/2018/01/15/lawyers-and-technology-frenemies-or-collaborators/#54a791ba22f1; Jon Tobin, *The Real Reason Why Lawyers Are Slow to Adopt Legal Technology*, MEDIUM (May 2, 2016), https://medium.com/@jontobinla/the-real-reason-why-lawyers-are-slow-to-adopt-legal-technology-1557c2adbe0a.

[41] *See, e.g.*, Robert J. Derocher, *Crisis in the courts: Bars take steps to stave off judicial funding cuts*, ABA BAR LEADER (2010),

very experimental methods of storing and preserving digital evidence will likely be a low priority, at least for the foreseeable future.

CONCLUSION

The increase in electronic transactions and record-keeping in the past few decades yielded amendments to the Federal Rules of Evidence to accommodate the increase in electronically-stored evidence. Similarly, the increase in blockchain-based transactions and record-keeping should—and, in time, likely will—spur the courts to make more changes to evidence rules, just as Vermont has done. Perhaps as courts become familiar with blockchain, both as evidence and for its record-keeping utility, we should expect to see more rules accounting for blockchain and its technical nuances.

---

https://www.americanbar.org/groups/bar_services/publications/bar_leader/2009_10/may_june/courtcrisis/; Peter T. Grossi, Jr. et al., *Crisis in the Courts: Reconnaissance and Recommendations*, NAT'L CTR. ST. CTS.: FUTURE TRENDS IN ST, CTS. (2012), https://www.ncsc.org/sitecore/content/microsites/future-trends-2012/home/Better-Courts/~/media/Microsites/Files/Future%20Trends%202012/PDFs/Crisis_Grossi.ashx.