



©iStockphoto.com/cnythzj

# Expert Q&A on Developing Issues in Blockchain Litigation

Blockchain technology burst into the public consciousness with the advent of bitcoin and other cryptocurrencies. More recently, the integration of blockchain into global commerce has presented numerous challenges and, predictably, has spawned litigation. As this powerful technology becomes increasingly affordable and commonplace, practitioners can expect blockchain-related litigation outside of cryptocurrencies to become more prevalent. Practical Law asked *Chuck Throckmorton* and *Daniel Maland* of *Kozyak Tropin & Throckmorton* to discuss key issues that litigators should consider when handling a blockchain-related case.



**CHARLES W. THROCKMORTON**  
OF COUNSEL  
KOZYAK TROPIN & THROCKMORTON

Chuck is a founding member of the firm and leads the firm's bankruptcy department. His practice focuses on bankruptcy, creditors' rights, and complex commercial litigation and appellate matters. Chuck has successfully represented numerous companies in Chapter 11 reorganizations and regularly represents lenders, secured and unsecured creditors, creditors' committees, and trustees in bankruptcy matters.



**DANIEL S. MALAND**  
ATTORNEY  
KOZYAK TROPIN & THROCKMORTON

Daniel is a member of the firm's complex litigation department. His practice focuses on representing both plaintiffs and defendants in bet-the-company litigation. Daniel's experience includes federal receiver representation, white collar criminal defense, and assisting clients with government investigations. He also consults on emerging technologies, with a focus on cybersecurity, blockchain, distributed ledger technologies, and smart contracts.

## What is blockchain, and how is it being implemented beyond its cryptocurrency origins?

Blockchain is a type of distributed ledger technology (DLT). The terms blockchain and DLT are often used interchangeably. At its most basic level, blockchain is a secure digital recordkeeping system that can be deployed on a limited or global scale. Once data is recorded on a blockchain ledger, it is encrypted and distributed across a network of internet-connected devices called nodes (such as computers, phones, or printers) that maintain a complete copy of the distributed ledger and validate new transactions or entries in real time.

Nodes regularly cross-check the accuracy of the data on the distributed ledger. If a single node has an entry that does not match that of the other nodes in the blockchain, the entry is rejected. Entries that the nodes approve for addition to a distributed ledger cannot be deleted once they are recorded, and only another accepted entry on the ledger can modify or correct a node.

Blockchain is inherently decentralized, meaning there is no single, centralized authority responsible for the distributed ledger. Due to its decentralized structure and cross-checking by nodes, blockchain is considered one of the most secure methods of recordkeeping developed to date.



Search [Glossary of Blockchain Terms](#) for definitions of key blockchain-related terms.

Blockchain has a range of uses and has rapidly evolved beyond its cryptocurrency origins. Indeed, blockchain technology is being developed and implemented across a wide spectrum, including by:

- **Financial institutions.** Blockchain technology is redefining the way banks conduct business. Financial institutions around the globe are committing substantial resources to developing their own blockchain systems to assist with processing financial transactions. (For more information on how financial institutions are using blockchain technology, search [Application of Distributed Ledger Technology to Financial Services Regulation and Compliance](#) on Practical Law.)
- **Private businesses.** Major industry leaders are partnering on blockchain-related endeavors to record and exchange information on a scale never before considered possible. For example, technology companies, food manufacturers, and retailers are coordinating on a blockchain technology dedicated to improving global supply chains and food safety. (For more information on the use of blockchain in the supply chain context, search [Blockchain and Supply Chain Management](#) on Practical Law.)
- **Governmental agencies.** For example, the Centers for Disease Control and Prevention has implemented a blockchain program designed to automate its compliance processes and revolutionize its tracking of health crises.

## At the outset of a blockchain-related case, what foundational information should counsel gather from the client?

When asked to handle litigation involving a blockchain issue, counsel should start by confirming the following details:

- **Whether the client's blockchain access is permissioned or public.** Counsel must understand who has access to and can modify the client's distributed ledger. Blockchain access can be permissioned (meaning access is restricted to only certain individuals who can modify the records) or public (meaning the public at large can access and modify the records). Many, if not most, distributed ledgers are permissioned for data privacy and security reasons. If the client's distributed ledger is permissioned, counsel should learn who has permission to view and make entries to the distributed ledger. This information is less of a concern if the client's distributed ledger is public (although public platforms present other issues).
- **Where the client's blockchain users and nodes are located.** After identifying the permissioned viewers and users, counsel should learn where those individuals are physically located and where the nodes for the distributed ledger are based or concentrated. These locations have regulatory and data privacy implications and may also impact the extraterritorial application of certain statutes.
- **Whether the client has smart contracts built into its blockchain platform.** A smart contract is a form of computer code that triggers self-executing transactions based on entries in the distributed ledger. It is essential to understand if the client has smart contracts built into its blockchain platform and, if so, whether any smart contracts have been improperly triggered. An entry recorded in error may inadvertently trigger a smart contract and create a chain reaction. If this occurs, counsel may need to seek expedited judicial intervention to protect the client. (For more information on smart contracts, search [Understanding Smart Contract Mechanics](#) on Practical Law.)
- **Who is best able to answer blockchain-related questions on behalf of the client.** As a recordkeeping system, a distributed ledger is discoverable and may need to be disclosed in a regulatory investigation or litigation. To effectively communicate and cooperate with opposing counsel and regulators on these matters, counsel should know in advance which client representative (whether an employee or a third-party consultant) is best equipped to discuss the client's blockchain technology. (For more information on regulatory investigations into blockchain activity, search [Blockchain Technology and Regulatory Investigations](#) on Practical Law.)


## What factors do courts consider when determining jurisdiction in disputes involving blockchain?

The geographic scope and scale of a blockchain system raises unique jurisdictional considerations. Generally, when determining personal jurisdiction over a nonresident defendant, federal courts will evaluate whether the defendant has either:

- A continuous and systematic presence within the forum state (known as general jurisdiction).
- Sufficient “minimum contacts” with the forum state such that the exercise of jurisdiction would not “offend traditional notions of fair play and substantial justice,” and the suit arises out of, or is related to, the defendant’s contacts with the forum state (known as specific jurisdiction) (*Int’l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) (internal quotations omitted)). A nonresident defendant may have minimum contacts with the forum state if it purposefully conducted activities in the state and took advantage of the benefits and protections of the state’s laws.

The nascent caselaw on this subject reflects that courts are weighing whether jurisdictional analysis regarding blockchain should differ from that used for other technology defendants, like e-commerce websites and cloud servers. In e-commerce cases, federal courts are reluctant to exercise personal jurisdiction based solely on the fact that a party hosts an interactive website on a server that is located in that forum and freely accessible by citizens of that forum. Courts generally hold that the mere presence of the website’s server in a forum does not automatically establish that the website’s owner is performing a commercial activity in that state. (See, for example, *Panavision Int’l, L.P. v. Toeppen*, 141 F.3d 1316, 1322 (9th Cir. 1998); *Savage Universal Corp. v. Grazier Constr., Inc.*, 2004 WL 1824102, at \*9 (S.D.N.Y. Aug. 13, 2004).)

Similarly, in considering personal jurisdiction in blockchain-related litigation, the location of blockchain nodes and data is not dispositive, and courts consider whether a defendant purposefully availed itself of the US, such as through widespread marketing of an initial coin offering (ICO) to US investors and use of employees in the US (see, for example, *Alibaba Grp. Holding Ltd. v. Alibabacoin Found.*, 2018 WL 5118638, at \*3-5 (S.D.N.Y. Oct. 22, 2018); *SEC v. PlexCorps*, 2018 WL 4299983, at \*10-19 (E.D.N.Y. Aug. 9, 2018); *In re Tezos Secur. Litig.*, 2018 WL 4293341, at \*6 (N.D. Cal. Aug. 7, 2018); see also *Shaw v. Vircorex*, 2019 WL 2636271, at \*2-4 (D. Col. Feb. 21, 2019)).

 Search [Commencing a Federal Lawsuit: Initial Considerations](#) for more on personal jurisdiction.

### How can counsel preempt potential discovery disputes relating to blockchain technology?

Counsel should develop and propose a formal, written protocol for discovery of electronically stored information (ESI). A detailed ESI protocol can help preempt disputes regarding the format in which a distributed ledger is produced during discovery, especially if it is produced only in part or with redactions. This is particularly critical for discovery of permissioned ledgers.

When drafting an ESI protocol, counsel should be mindful of the court’s local rules regarding production formats. While certain jurisdictions permit files to be produced in their native format, others require more. For example, the US District Court for the District of Delaware requires that both ESI and non-ESI be

produced as text searchable image files (DE R USDCT Discovery Standard § 5(c)). However, if a party keeps corporate records (such as stock ledgers) on a distributed ledger, Delaware also requires that these records be convertible into a clearly legible paper form within a reasonable time (8 Del. C. § 224).

Counsel should also recognize that production of a full distributed ledger may not be necessary or appropriate. Counsel should consider whether an opposing party’s discovery request contravenes Federal Rules of Civil Procedure 26(b) and (g), which require the scope of discovery to be reasonable, relevant to a claim or defense, and proportional to the needs of the case.



Search [Document Production Protocols in Federal Civil Litigation](#) for more on developing a protocol to establish parties’ rights and obligations when producing documents and ESI in discovery.

Search [Making and Responding to Proportionality Objections](#) for more on proportionality-based objections in federal civil discovery.

### Are distributed ledgers admissible as evidence at trial?

Some states in the US have enacted legislation and taken other steps to address the validity and admissibility of blockchain evidence. These states include:

- **Vermont.** In 2016, Vermont passed H. 868 (Act 157), which establishes that a “fact or record verified through a valid application of blockchain technology is authentic” and admissible under the Vermont Rules of Evidence (12 V.S.A. § 1913). Under this legislation, blockchain records are admissible over hearsay objections when those records are accompanied by a written declaration of a qualified person that testifies to the details of the distributed ledger transaction.
- **Delaware.** In 2017, Delaware passed Senate Bill 69, which authorizes corporations to maintain their required lists of shareholder names using blockchain technology rather than in spreadsheet or traditional database form (8 Del. C. § 224).
- **Tennessee.** In 2018, Tennessee passed Senate Bill 1662, which recognizes the legal authority to use blockchain technology and blockchain contracts in electronic transactions (T.C.A. § 47-10-202).
- **Arizona.** In 2017, Arizona passed House Bill 2417, which establishes that signatures obtained through blockchain technology are valid and binding (A.R.S. § 44-7061).

Several other states have formed working groups to explore the use of blockchain technology by state government agencies for recordkeeping purposes. These states include:

- California.
- Florida.
- Hawaii.
- Illinois.
- Maine.
- North Dakota.

Even absent blockchain-specific legislation, the Federal Rules of Evidence (FRE) provide sufficient means for admitting

## BLOCKCHAIN TOOLKIT

The Blockchain Toolkit available on Practical Law offers a cross-practice collection of resources on blockchain-related topics, such as smart contracts, digital assets, cryptocurrency, and ICOs. It includes:

- [Blockchain Legal Update Tracker](#)
- [Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues](#)
- [Understanding the SEC's Digital Asset Framework and Approach to Digital Asset Regulation](#)
- [FinCEN Guidance on Virtual Currency Compliance: Overview](#)
- [Security Interests: Bitcoins and Other Cryptocurrency Assets](#)
- [Blockchain and Distributed Ledger Laws: State-by-State Adoption](#)
- [Blockchain Antitrust Considerations Checklist](#)
- [Fintech in the Banking Industry: Legal and Regulatory Issues](#)
- [Blockchain Cash Issuer Q&A with R3 Legal Center of Excellence](#)
- [Expert Q&A on Retirement Plans and Blockchain](#)

distributed ledger entries as evidence. Parties may need both expert and lay witnesses to authenticate ledger records and lay the proper foundation for the records to be admitted. By presenting experts who can explain the meaning of entries on a ledger in layman's terms, counsel may be able to admit this blockchain evidence in the face of evidentiary objections, such as those based on hearsay (FRE 802), the best evidence rule (FRE 1002), or failure to authenticate (FRE 901).



Search [Expert Toolkit](#) for a collection of resources to assist counsel with the use of experts in federal civil litigation.

Search [Evidence in Federal Court: Overview](#) for more on hearsay, the best evidence rule, authentication, and other rules governing the admissibility of evidence.

### Have any courts directly addressed evidentiary issues concerning blockchain?

Courts around the world are starting to accept distributed ledgers as admissible evidence. For example, China's Supreme People's Court now recognizes blockchain-authenticated evidence in China's Internet Courts. These special trial courts have recently been set up in select Chinese jurisdictions to handle disputes involving the online sale of goods and services, lending, domains, and infringement on personal rights or property rights via the internet, among other matters.

Although no US court has specifically addressed the admissibility and authentication of blockchain evidence, recent caselaw on the admissibility of machine statements offers a preview of how evidentiary issues concerning blockchain might play out. For example, in *United States v. Lizarraga-Tirado*, the Ninth Circuit ruled that a Google Earth image showing a pinpoint of the defendant's location could be admitted as evidence, despite an objection that the satellite image on its own and the digitally added "tack" labeled with GPS coordinates were impermissible hearsay. After finding that the satellite

image did not constitute hearsay because it merely depicted a scene as it existed at a particular time and did not make an "assertion," the court noted that the tack and coordinates presented "a more difficult question" because labeled markers assert that the labeled item exists at the location of the marker.

In concluding that the tack and coordinates did not constitute hearsay, the court reasoned that, because Google Earth generated the tack and coordinates automatically, the relevant assertions were made by a program and not a person. The court further explained that:

- Concerns that a machine might malfunction, produce inconsistent results, or have been tampered with should be addressed by the rules of authentication and not hearsay.
- When faced with an authentication objection, a proponent of Google Earth-generated evidence would need to establish Google Earth's reliability and accuracy through, for example, testimony from a Google Earth programmer or a witness who frequently works with and relies on the program. (This reasoning echoes Vermont's new blockchain legislation discussed above.)

(*Lizarraga-Tirado*, 789 F.3d 1107, 1109-10 (9th Cir. 2015); 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 and concluding that they were).)

The same procedure and analysis could be extended to blockchain technology. While a person can make an entry on a distributed ledger, a ledger can also be updated via coded requests without human involvement, such as through smart contracts. As the *Lizarraga-Tirado* case illustrates, courts will likely be open to arguments that the accuracy of authenticated ledger entries cannot reasonably be questioned because, like the digital tack in that case, the court will be able to "accurately and readily determine" that a ledger entry was made automatically via computer programming (789 F.3d at 1109).