APRIL 3, 2019

Legaltech® news

ONLINE

An ALM Publication

Emerging Discovery Issues in Blockchain Litigation

BY STUART D. LEVI, ALEXANDER C. DRYLEWSKI, GIYOUNG SONG AND THANIA CHARMANI, SKADDEN

The increased use of blockchain technology and, in particular, cryptocurrencies, has given rise to a variety of disputes, including government enforcement actions and private litigation. Substantive issues regarding the offer, sale and trading of digital tokens are coming before the courts, prompting novel discovery questions in these cases.

Blockchain Litigation

Blockchain technology is a distributed ledger system that allows for the creation of secure and presumably immutable records. Certain blockchains are public and permissionless, allowing anyone to join, while others are private and only accessible by permissioned users (e.g., banks). To date, most applications of the technology have been to record transactions, including those involving digital assets such as cryptocurrencies.

Depending on the circumstances, some digital assets may be subject to regulation by the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the U.S. Treasury Department, federal banking regulators, and/or state and foreign regulators.

In an effort to regulate certain digital assets and related transactions, the SEC and CFTC each have taken a number of enforcement actions, including filing complaints and cease-and-desist proceedings against promoters of initial coin offerings, fund managers investing in digital assets, and decentralized exchanges in which coins and tokens can be traded.

Private cryptocurrency litigation has mostly involved class action complaints filed by plaintiffs purporting to represent investors who bought a particular cryptocurrency, alleging securities violations and various state law claims.

Potential Discovery Issues in Blockchain Cases

The increase in litigation involving blockchain technology may give rise to issues of first impression in the discovery context as courts apply existing principles to the unique characteristics of blockchain technology, including the discovery of information that is public and transparent, the decentralized and immutable nature of blockchain transactions and the use of "smart contracts" to execute transactions.

Transparency: One novel aspect of blockchain technology is that transaction records are transparent, and thus viewable to all, and decentralized, meaning that, for public blockchains, there is no central governing or managerial body. Since no party is in "possession, custody or control" of transaction records, a party receiving a discovery request for such information might have legitimate grounds for objecting.

However, this is not always the case. Many blockchain projects involve data stored on a blockchain as well as "off-chain." This could yield discovery battles concerning where the line is drawn and what information a party actually controls.

In addition, the parties to blockchain transactions are anonymous or

"pseudonymous," such that the identities of transacting parties generally are not publicly available. Rather, the public can only see wallet addresses engaged in the transaction, while third parties may hold information linking wallets to identity. As a result, plaintiffs and enforcement agencies have sought discovery of ownership information.

For example, in *Paige v. Bitconnect Int'l PLC* plaintiffs accusing a cryptocurrency exchange of operating a Ponzi scheme were permitted to obtain disclosure of all cryptocurrency wallet addresses, trading account addresses and the identity of account holders. Similarly, in *United States v. Coinbase, Inc.*, the court ordered a digital exchange to provide the IRS with information regarding account holders' identities to the extent the account holder had a taxable gain.

Immutability: When engaging in discovery, parties generally are mindful of the ultimate admissibility of relevant evidence, and another issue of first impression may be the admissibility and authenticity of blockchain records at

trial. Because blockchain records are meant to be immutable they are arguably more reliable than other data sources and could provide an indisputable chain of custody.

While courts have not addressed the admissibility of blockchain records specifically, such records would likely qualify as computer-generated information that can be self-authenticated under Rule 902 of the Federal Rules of Evidence, provided that the party seeking introduction can submit a written certification from a qualified person. Indeed, the state of Vermont has enacted a statute permitting blockchain records to be authenticated and admitted when accompanied by a written declaration of a qualified person, unless there is an indication of a lack of trustworthiness.

Blockchain records also may be deemed analogous to statements or information generated by computers, which some courts, such as in *United States v. Lizarraga-Tirado*, have held do not constitute hearsay. Interesting questions may arise regarding the accuracy or completeness of information reflected on a distributed ledger in light of potential evidence of "off-chain" transactions and so-called "forks" in the ledger based on errors and other events.

Jurisdiction: Because blockchain networks are decentralized, they generally involve a limitless number of computers globally distributed. Accordingly, these networks may not have a presence, or involve parties engaging in activities, in any one physical location. Therefore, blockchain litigation may involve questions around personal jurisdiction, extraterritorial application of U.S. laws, and judgment collection, and jurisdictional discovery may be sought where these issues arise.

In some cases, courts are able to navigate disputes over jurisdiction where a party is an identifiable "on-ramp" to a blockchain or where the conduct at issue occurred before full decentralization took place. For example, in the *Tezos* securities litigation, the court held that the defendant was subject to personal jurisdiction based on factual allegations that the websites were in English, hosted in the U.S., and the offering was designed to accommodate U.S.-based participation. In finding there was proper extraterritorial application of the Securities Exchange Act of 1934, the court considered where the website was hosted and operated, and whether "a network of global 'nodes'" in the blockchain were "clustered more densely in the United States than in any other country."

On the other hand, a Colorado federal court in *Shaw v. Vircurex* recently dismissed on personal jurisdiction grounds a class action brought by an investor in a defunct online digital currency exchange after its operators allegedly froze customer funds while descending into insolvency. The court held there was no evidence that the account process involved any negotiations (which, in a traditional transaction, would have taken place at least in part in Colorado) or that the defendants purposefully directed their activities at Colorado or even knew that the injury would be felt there.

Smart Contracts: Going forward, many blockchain transactions will be conducted using "smart contracts," or pieces of code that automatically effectuate transactions on a blockchain, such as moving funds upon certain triggering events.

The use of smart contracts, and disputes arising therefrom, may create novel discovery issues relating to the contracting parties' intent and what steps the code actually executes. Unlike traditional contracts, the "drafter" of a smart contract generally is a third-party programmer that may not be involved in any other way in the transaction at issue.

Litigants will thus need to consider how to obtain (and ultimately present in court) admissible evidence regarding what might otherwise be straightforward issues of contract interpretation, including whether to rely on technical experts or other third parties to explain how the parties' agreement is accurately reflected in a given smart contract's code. Furthermore, as non-programmers may struggle to understand even the most basic smart contract, litigants may need to rely more heavily on expert discovery to explain how the smart contract operates and the manner in which its program carried out the parties' supposed agreement.

Stuart D. Levi *is co-head of Skadden's Intellectual Property and Technology Group, and he coordinates the firm's blockchain, outsourcing and privacy practices. He has been a recognized leader in the technology transaction field for over 30 years and in 2018 was recognized as a National Law Journal Trailblazer in cryptocurrency, blockchain and fintech.* ***Alexander C. Drylewski*** *focuses on securities and complex commercial litigation in state and federal courts throughout the country. He represents corporations, financial institutions and individuals across a wide range of industries in a variety of disputes, including all facets of commercial litigation, securities class actions, shareholder derivative lawsuits, and federal and state appeals.* ***Giyoung Song*** *represents financial institutions, corporations and individuals in complex litigation and investigation involving corporate, commercial, bankruptcy, antitrust and securities-related matters in federal and state courts.* ***Thania Charmani*** *is an associate in Skadden's Complex Litigation and Trials group.*