Bloomberg Law®

BNA's
Patent, Trademark & Copyright Journal®

Extraterritoriality

Enforcing U.S. Patents on Blockchains Distributed Worldwide

Extraterritoriality

Those seeking to protect their blockchain IP should consider including at least one system claim in their patent application and also expressly identifying the benefits flowing from each element of the system that are directed to a potential infringer, write Salvatore P. Tamburo, Ameya V. Paradkar, and Ji Young Park of Blank Rome LLP. Those accused of infringing a blockchain system claim may find success in arguing that the purported direct infringer does not garner a benefit from each element of the system claim, or that the purported benefit is, at best, cumulative to the system, they write.



By Salvatore P. Tamburo, Ameya V. Paradkar, and Ji Young Park

As blockchain technology finds applications beyond cryptocurrencies, various use cases are emerging. Blockchain has the potential to form the backbone of next-generation payment systems and to serve as critical infrastructure for a ubiquitous, worldwide exchange platform. Given the potential to rewrite how businesses conduct commerce, the sudden great interest in blockchain patents is not surprising. Generally speaking, however, U.S. patents may be enforced only against infringing systems located within the U.S. A system supported by blockchain technology, however, may be implemented across various countries including the U.S., implicating an area of patent law known as extraterritoriality. This article examines how extraterritorial activities common in implementing blockchain technology may have unintended consequences on the enforcement of these new blockchain patents. Conversely, extraterritoriality may offer a welcome defense to those accused of infringing a blockchain patent.

Blockchain, in its simplest form, is a decentralized ledger technology, in which virtually anyone with a computing device may verify and record transactions online. The verifying and recording of the transactions are performed according to a predetermined set of rules. These rules include how to cryptographically hash a proposed transaction and derive a new block of data based on the hashed transaction. The new block is then added to the existing chain of blocks to record the transaction.

 ISSN 0148-7965

In the blockchain world, the rules governing the verification and recording of transactions are usually set by a person, group, or entity, who begins the block. For the purposes of this article, they are referred to as the ''managing entity.'' Those who verify and record transactions are known as ''miners.'' Most popular blockchains — for example, the Bitcoin network — allow anyone with a computing device to become a ''user'' and conduct transactions, which are verified and recorded by ''miners'' on the blockchain network according to the rules set by a ''managing entity.'' For more background on blockchain technology, see *Divided Infringement: Weak Link in Secure Blockchain IP Strategy*?

Because of their decentralized nature, blockchains — and their users, miners, and managing entity — are spread around the world. While enabling borderless transactions among users in various countries is one of the most powerful features of the blockchain network, it also raises questions regarding whether a U.S. patent covering blockchain technology may be enforced when at least part of the network is located outside of the U.S. The U.S. Court of Appeals for the Federal Circuit, the appellate court of first instance for all patent matters, provides some guidance for such circumstances.

In *NTP, Inc. v. Research In Motion, Ltd.*, 418 F.3d 1282 (Fed. Cir. 2005), Research In Motion's BlackBerry wireless email system was accused of patent infringement. An email sent by a BlackBerry system user in the U.S. traveled through a relay in Canada before reaching its destination. RIM argued that because the relay was outside of the U.S., it cannot be liable for patent infringement under 35 U.S.C. § 271(a), which requires ''use'' of the patented invention to occur ''within the United States.''

The Federal Circuit recognized, however, that the statutory language is unclear where a component or a step of the patented invention (as contrasted with the entire invention) is located or performed abroad. The Federal Circuit further found that other courts have interpreted the term ''use'' broadly as to ''put into action or service.''

Against this backdrop, the Federal Circuit held that a patented system is in ''use'' under Section 271(a) — even if a component of the system is located outside the U.S. — as long as the system *as a whole* was put into service in the U.S., *i.e.*, control of the system was exercised in and the beneficial use of the system was obtained in the U.S. In RIM's case, because its customers (i.e., the direct infringers), located within the U.S., controlled transmission of the information that traveled through the Canadian relay, and benefited from such an exchange of information, the relay's location did not preclude infringement of the system claim.

The court, however, held the opposite regarding the use of a patented method. Unlike the use of a system, in which the components are used collectively, the use of a process necessarily involves doing or performing each of the steps recited. Accordingly, a process cannot be used ''within'' the U.S., as required by Section 271(a), unless each of the steps is performed within the U.S. In *NTP*, because one of the steps of the asserted method claim could only be satisfied by using the Canadian relay, the court found that the claimed method could not be infringed by using the BlackBerry system.

Given this legal framework, and given the extraterritorial nature of blockchain technology, system claims covering this technology may be found to infringe while method claims may not. This is true even if both sets of claims are directed toward the same invention.

Consider the following exemplary claim, directed to a generic blockchain method:

- A method for recording transactions on a distributed network comprising,
  - submitting one or more proposed transactions to the distributed network;
  - providing a cryptographic algorithm to hash the submitted transactions;
  - cryptographically hashing the submitted transactions based on the provided algorithm;
  - verifying the hashed transactions; and
  - recording the verified transaction in one or more databases.

If even just one of the above steps were not performed within the U.S., such as the verification (e.g., performed by a miner) or recording step (e.g., performed by a managing entity), under *NTP*, there can be no infringement.

However, if the same invention were claimed as a system instead of a method, the results could be different. Consider the following exemplary system claim:

- A system for recording transactions on a distributed network comprising,
  - a plurality of networked computers to which a proposed transaction is submitted;
  - a first processor for cryptographically hashing the submitted transactions based on a cryptographic algorithm;
  - a second processor for verifying the hashed transaction; and
  - a database for recording the verified transaction.

Here, infringement under Section 271(a) may be found even if one of the elements of the system is operated outside of the U.S. as long as the control of the system is exercised in and the beneficial use of the system is obtained within the U.S.

But how does a patentee establish that control was exercised and beneficial use was obtained in the U.S.? Two more recent Federal Circuit decisions provide guidance.

In both *Intellectual Ventures I LLC v. Motorola Mobility LLC*, 870 F.3d 1320 (Fed. Cir. 2017), and *Centillion Data Sys., LLC v. Qwest Commc'ns Int'l, Inc.*, 631 F.3d 1279 (Fed. Cir. 2011), the issue was whether an end user of a patented system not entirely physically under the end user's control can nonetheless be found to control and benefit from the system, thereby infringing the patent. In *Centillion*, the Federal Circuit found that an end user controlled a back-end component of a system, even though the back-end component was not physically under his control, because, absent a user request to the back-end component using a front-end component that *was* within his physical control, the back-end component would not be put into service (the direct or indirect control required ''is the ability to place the system as a whole into service''). By causing the system as a whole to operate as patented and by obtaining the benefit of the result, the Federal Circuit found that the end user ''used'' the patented system as a matter of law.

In *Intellectual Ventures I LLC*, the Federal Circuit further clarified that an infringer must not only control but also benefit from *each element* of the claim. 870

F.3d at 1329. The claim at issue in *Intellectual Ventures I LLC* recited, *inter alia*, ''an authentication device'' configured to ''generate a delivery report.'' The alleged direct infringer, an end user of Multimedia Messaging Service, did not maintain or operate the Multimedia Messaging Service Centers corresponding to the authentication device: it was instead maintained and operated by the end user's wireless service carriers. Because there was no evidence that the end user's device received the delivery reports generated by the carriers, which was the only benefit identified as flowing from the delivery reports in the asserted patent, the end user was not found to have benefited from the authentication device's generation of delivery reports. Thus, the end user did not infringe the patent.

Applying these holdings to the exemplary system claim above, a blockchain patentee could likely argue that a user of the blockchain network in the U.S. is infringing by causing the system as a whole to operate. Had it not been for the user's submission of the proposed transaction to the distributed network, the entire system would not have been put into use. When the proposed transaction is submitted to the distributed network, every element of the system is used regardless of its geographical location. And under *Intellectual Ventures I LLC* and *Centillion*, a user of the blockchain network arguably controls the use of each claim element in the U.S.

Whether the user benefited from each element of the claim in the U.S., however, may be a more fact-specific inquiry. Although a patentee may argue that the user is benefiting by being able to use the system to conduct an online transaction, *Intellectual Ventures I LLC* rejected a similar argument that the user simply has to obtain benefit from the system as a whole. Rather, a patentee must show that the user benefited from *each* claimed component of the system.

In view of the present legal posture on extraterritoriality, those seeking to protect their blockchain IP should consider including at least one system claim in their patent application and also expressly identifying the benefits flowing from each element of the system that are directed to a potential infringer. For example, the specification of the patent could identify possible benefits to a U.S. blockchain user from each claim element, *e.g.*, the ''plurality of networked computers'' might allow the user to use the system regardless of its geographical location within the U.S.; the ''first processor'' and ''second processor'' might allow the user's transaction to be hashed and protected against cyberattacks; and the ''database'' might allow the user's transaction to be preserved and accessible in the future for further transactions.

Conversely, those accused of infringing a blockchain system claim may find success in arguing that the purported direct infringer does not garner a benefit from each element of the system claim, or that the purported benefit is, at best, cumulative to the system. Extraterritorial doctrine may thus prove a useful tool in a defendant's arsenal, short-circuiting a case at an early stage. By understanding how the extraterritorial activities of a blockchain network affect the enforcement and defense of blockchain patents, inventors can better prepare their patent applications to address these potential roadblocks that may affect the efficacy of their patents.