Bloomberg Law

BNA's
Patent, Trademark
& Copyright Journal®

Infringement

Divided Infringement: Weak Link in Secure Blockchain IP Strategy?

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

Blockchain is familiar to most as the foundational technology for cryptocurrencies such as Bitcoin. But current applications and future potential of blockchain are much more far-reaching, with applications in finance, health-care records, and smart contracts just to name a few. As blockchain is becoming more prevalent, many corporations are obtaining patent protection for these new technologies and applications. This article examines how the doctrine of divided infringement — which dictates that only a single actor may infringe a patent — can potentially affect the enforcement and defense of these new blockchain patents.

Salvatore P. Tamburo, a Washington-based partner at Blank Rome LLP, specializes in patent litigation in various technologies, including authentication software.

Ameya V. Paradkar, a Washington-based associate at Blank Rome LLP, concentrates his practice on patent litigation and counseling in software related to authentication, data streaming, and machine learning, as well as biotechnology.

Ji Young Park, a Washington-based associate at Blank Rome LLP, concentrates her practice on patent litigation and counseling in telecommunication standards, networking systems, and machine learning.

Technological Background

Blockchain technology is premised on the pillars of a decentralized, distributed ledger and a multiparty trust network to amend and update that ledger. The blockchain ledgers, located at nodes of the network, act as a real-time master record of all transactions occurring in the network. The nodes are computers that store a copy of the ledger and may participate in transaction verification. Updates to this ledger are possible only by the mutual consent of the nodes of the network.

Because the integrity of the blockchain network depends on the veracity of the ledgers, multiple miners of the network can only add to the ledgers after the application of specific cryptographic protocols and verification. Once the network agrees to add to the ledger, the ledger is updated across all nodes of the blockchain. As multiple instances of the ledger exist in the network, hacking the records of a single ledger is ineffective in compromising the integrity of the network.

In general, transactions are proposed for entry into the ledger without identifying the users participating in the transaction. Users are those members of the blockchain that engage in transactional activity on the network. New proposed transactions are grouped together and fed through a cryptographic hash function that is combined with the previous block's header and time stamp to create a new header, which is appended to the new proposed transactions. This new header acts as a puzzle for the nodes of the blockchain network to solve. This puzzle can only be solved using brute-force calculations that apply the cryptographic hash function. The nodes typically race against one another to solve the header puzzle.

Once a node arrives at a solution, other nodes in the network check the result. Typically, the nodes are incentivized to perform these computations, for example, through tokens or cryptocurrency. In those cases, the nodes may be referred to as ''miners.'' Once a certain number of nodes confirm the solution for the header puzzle, those new transactions associated are added to the blockchain ledger across all of the nodes. This is referred to as adding a ''block'' to the blockchain. The header from this new block is then used in subsequent iterations to add to the blockchain.

Blockchain has a number of applications in such varied fields as finance, health care, and information technology. Indeed, any industry that relies on database integrity can apply blockchain to reduce costs and increase efficiency. In the case of cryptocurrency, the blockchain transactions take the form of ''coins'' or ''tokens,'' whose values are determined on the open market. In the case of blockchain networks involving smart contracts, the transactions in question are instead agreements, typically with a standardized set of provisions, which are verified and added to the decentralized ledger. Such a blockchain is particularly useful in the verification of trades between counterparties on the financial markets. Although cryptocurrency may be the application *du jour*, it is other forms of blockchain that may ultimately find the most utility as the technology matures.

Blockchain and Divided Infringement

As blockchain technology becomes increasingly mainstream, corporations developing their own blockchains are pursuing an aggressive strategy to protect their intellectual property. The U.S. Patent and Trademark Office database showed more than 550 U.S. published patent applications related to blockchain as of February 2018. Many more are likely to publish in the coming months. The inherent decentralization of blockchain, however, creates notable issues under prevailing patent law, including, for example, divided infringement. Depending on how a patent claim is drafted, it may implicate the actions of a single entity and avoid divided infringement issues. Divided infringement may occur, however, when more than one person or entity is required to infringe a patent claim. From a patentee's perspective, ideally, a patent claim is infringed by a single entity. This type of infringement simplifies the evidentiary showing required to demonstrate infringement, because only a single entity's actions must be analyzed against the claim language. Blockchain technology, however, inherently relies on multiple entities to perform certain steps. For example, verifying a proposed transaction and deciding to add that transaction to the ledger may require the performance of multiple parties.

Akamai Techs., Inc. v. Limelight Networks, Inc., 797 F.3d 1020 (Fed. Cir. 2015) (*en banc*), articulates the Federal Circuit's present posture on divided infringement. In *Akamai*, the court determined that it ''will hold an entity responsible for others' performance of claim limitations in two sets of circumstances: (1) where that entity directs or controls others' performance, and (2) where the actors form a joint enterprise.'' *Id.* at 1022. The ''control and direction'' analysis is a fact-specific inquiry, where ''liability [for infringement] can [ ] be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance.'' *Id.* at 1023. A number of factors are considered, including the signing of a standard contract, a welcome letter, instructions for use, assignment of user identifiers, installation guides, and provisioning of technical assistance. *Id.* at 1024-25.

The court also stated that finding a ''joint enterprise'' requires a showing of four elements: ''(1) an agreement, express or implied, among the members of the group; (2) a common purpose to be carried out by the group; (3) a community of pecuniary interest in that purpose, among the members; and (4) an equal right to a voice in the direction of the enterprise, which gives an equal right of control.'' *Id.* at 1023. Depending on the particular facts, a joint enterprise may be found, for example, when a group of banking institutions form their own closed blockchain network to clear financial transactions or when a corporation creates a closed blockchain network to store employee records. In these cases, the banks and corporations operate as both the managing entities — the entities overseeing the particular blockchain network — and the nodes.

In cases where access to the blockchain is not closed, a party defending against a claim of patent infringement may need to show that it does not condition participation in an activity or receipt of any benefits on the performance of a claim limitation, and that it does not control the manner or timing of the performance of that limitation.

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

A method to record 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 transactions in one or more databases.*

In the above claim, a user in the network performs the first step, submitting transactions into the network. The managing entity performs the second step of the method, providing the cryptographic hashing protocols. The third and fourth limitations, the actual hashing and verifying of the transaction, are performed by yet another entity, for example, miners at nodes in the blockchain network. Both miners and the managing entity may perform the final step of the method, recording the verified transaction to the blockchain. Because this sample claim requires the actions of multiple entities or users, divided infringement would be an issue.

As shown below, however, it is possible to draft a claim that would implicate only a single actor. This exemplary generic claim is directed to only the activities of a managing entity.

A method to record transactions on a distributed network comprising:

- *receiving one or more proposed transactions in the distributed network;*
- *providing a cryptographic algorithm to hash one or more submitted transactions, wherein said transactions are hashed in the distributed network using the algorithm;*
- *providing a predetermined valuation for verifying the hashed transactions, wherein tokens are allocated within the distributed network based on the predetermined valuation; and*
- *recording the verified transactions in one or more databases*.

As is apparent from the above, in general, patent claims directed to the verification of a proposed addition to the blockchain and additions of blocks to the ledger should alert patent litigators to a potential divided infringement issue. Verification, which is generally performed by nodes in the network, may be considered outside the direction and control of the managing entity depending on the particular facts. For example, one could argue that, under *Akamai*, the managing entity may have little control over the manner or timing of verification. Similarly, due to the decentralized nature of the blockchain ledger, a managing entity may not necessarily add verified blocks to the chain. Rather, upon verification, the ledgers may be updated by the nodes maintaining the blockchain. As a result, depending on the particular facts, the manner and timing for both verifying and adding blocks to the decentralized ledgers may be found to be outside the direction and control of the managing entity.

Moreover, because most current blockchain networks are inherently collaborative, rather than paternalistic, those running its nodes generally do not sign standardized contracts with the managing entity. Furthermore, the nodes usually choose their own anonymous identifiers, which are typically unknown to any participant in the network. As a result, a managing entity is unlikely to provide substantive documentation or support to its participants, all of which can weigh against a finding of direction and control, or a joint enterprise, under *Akamai*.

As its value to user privacy and transaction verification come into focus, blockchain appears poised to become pervasive. With such high attributable value, thousands of patents and applications should be expected in the coming years. As demonstrated above, the decentralized nature of blockchain means that it is inherently susceptible to divided infringement issues. These divided infringement issues may create unwanted complications from a patentee's standpoint or welcome defenses from an accused infringer's standpoint. Those considering patent protection directed to blockchain should consult with a patent attorney familiar with the technology to ensure the best chance of steering clear of such issues for enforcement. And those accused of infringement would be well-advised to strongly consider divided infringement, and its required evidentiary showings, as a defense to blockchain patents.