TOP INTELLECTUAL PROPERTY LAWYERS

Testing the cryptocurrency patent waters

Shutterstock

By Darin Snyder and Tony Beasley

Bitcoin and other cryptocurrencies went from confusing curiosities to mainstream topics in 2017. Before they became regular headlines, the paradigm-shattering possibilities of this technology brought a flood of patent filings on anything and everything that might touch it, including trading platforms, transfer methods, processing loans using distributed ledgers, and even cryptocurrency-based voting systems. Analysis of some of these applications already confirms the critical importance of disclosing a tangible, meaningful improvement to computing technology as part of the invention.

The rapid staking of cryptocurrency patent territory has challenged the notion of what is allowable subject matter and what isn't under 35 U.S.C. Section 101. While no federal district court has yet scrutinized any such patent, battles have been and are currently being fought at the U.S. Patent and Trademark Office over whether cryptocurrency inventions are valid under Section 101. These battles have run in parallel with the U.S. Court of Appeals for the Federal Circuit's recent rulings on subject-matter eligibility, including especially *Enfish LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016), and *McRO, Inc. dba Planet Blue v. Bandai Namco Games America Inc.*, 837 F.3d 1299 (Fed. Cir. 2016).

The PTO has made clear that reciting the use of cryptocurrency in a patent application will not, alone, render the invention subject-matter eligible. Examiners have specifically stated, for example, that "[t]he concept of electronic money is [] well-known, routine and conventional" and that "cryptocurrency itself is an abstract concept." Where patentability lies, instead, is in the improvements to the technology on which cryptocurrency applications function. As has been shown by several applicants, the ability to overcome Section 101 rejections is tied directly to the ability to embody these improvements in specific claim limitations and advocate the meaning and import of these limitations.

Two recent patents illustrate this concept. The first, U.S. Patent No. 9,836,790 ("the '790 Patent"),

assigned to Bank of America Corp. (which accounts for over 5 percent of all cryptocurrency-related patent filings), shows the importance of skilled advocacy before the PTO in showing meaningful improvements to the security of cryptocurrency-based transactions. The second, U.S. Patent No. 9,747,586 ("the '586 Patent"), assigned to CPN Gold B.V., further exemplifies both advocating for technological improvements and explaining the difference between cryptocurrency-related claims and known, cryptocurrency-related concepts.

Bank of America's '790 Patent

The '790 Patent — "Cryptocurrency transformation system" — issued on Dec. 5, 2017. It claims a system that can receive electronic requests to exchange currency (e.g., U.S. dollars) for cryptocurrency (e.g., bitcoin), determine an optimal rate for the exchange, and then perform the exchange through the use of temporary, or "float," accounts on the banking system.

The '790 patent endured a roughly 2.5-year application process at the PTO that included three rejections under Section 101. The first and second Section 101 rejections noted that the claims were impermissibly abstract because they were drawn towards a currency exchange, which is a "fundamental economic practice" and required "no more than a generic computer to perform generic computer functions" and because the '790 claims improved only the "abstract idea of currency exchange" while using computers as tools.

In amendments to the claims, the '790 applicants first added requirements that the cryptocurrency exchange use "a cryptocurrency private key associated with a float account" and that it securely store this key by generating "vault keys" that were then themselves stored in two separate locations. The applicants later added limitations requiring that the vault keys be generated by applying hash functions (i.e., processes by which a potentially large amount of data is input to produce a fixed-length value) to different portions of the cryptocurrency private keys, which allows the cryptocurrency owners to access the currency. The applicants relied on McRO to argue that the amended '790 claims "positively recite[d] and articulate[d] specific rules that achieve an improved technological result."

These arguments and amendments were successful, and the claims were allowed. The resulting system of the '790 Patent is a cryptocurrency exchange that not only facilitates the exchanges but also uses public/private key pairs and hash functions to securely store and protect the cryptocurrency private key. The layering of these security measures on top of the baseline system, and the skilled advocacy regarding the

import of these added measures, resulted in a tangible technological improvement in the emerging field of cryptocurrency exchanges and an issued patent.

CPN Gold's '586 Patent

The '586 Patent is titled "System and method for issuance of electronic currency substantiated by a reserve of assets" and issued on August 29, 2017. It claims a system for managing cryptocurrency wallets and related information about a "reserve," specifically of gold, that substantiates the cryptocurrency in real time. The '586 Patent endured two rejections under Section 101, both of which noted that the claims do not require anything more than non-conventional computer components and that the recited concepts "do not amount to significantly more than abstract ideas."

The '586 applicants responded to these rejections by adding several limitations requiring, for example, real-time monitoring and control of the substantiation of the electronic currency by a gold reserve (as opposed to any tangible asset). The applicants also described several differences between their claims and the cryptocurrencies known in the art, such as bitcoin. For example, the applicants argued that their claims require a private blockchain, which improves security over a public blockchain that uses a shared ledger. Another difference: the applicants' claims generate currency from a single block rather than through mining operations that act upon the entire blockchain, as is the case with bitcoin, and are slower. The claimed currency generation can "issue currency as necessary based on the relative demand by clients" and avoids the potential bottleneck that might result from blockchain mining not meeting demand for the currency. These amendments and arguments ultimately resulted in the issued '586 claims.

These patents are merely two examples of cryptocurrency patents and the applications they cover. Such applications will be patentable in light of the current state of Section 101 jurisprudence as long as applicants can skillfully identify a tangible, meaningful improvement to the computing technology described in and resulting from the invention.

Darin Snyder *is a partner at O'Melveny & Myers LLP who serves as regional head of Litigation for Northern California and on the firm's Policy Committee. His practice focuses on major litigation and investigations involving intellectual property and technology-intensive business sectors.*
Tony Beasley *is counsel at O'Melveny who focuses his practice on intellectual property litigation and has experience in many areas of technology.*