Protecting blockchain and cryptocurrency tech

John Carlin and **Doug Sharrott** explain best practice for protecting blockchain inventions

It's been said that blockchain may "prove to be one of the most disruptive innovations of the 21st century"[1] and "change the world".[2] The technology is now being applied to various lines of business as its usefulness becomes increasingly recognised.

Over the past four years, there has been a rush to invest in new cryptocurrencies and patent various aspects of blockchain technology. There are many reasons stakeholders are seeking patent protection for such developments. One operating company is less likely to sue another for patent infringement if the competitor also has patents it can assert in response.

Blockchain, a database of identical blocks of data distributed on a network of peer-to-peer computing nodes, reduces the risk of single-point failure and preventing control by a single entity. It maintains a continuously growing list of ordered records that are securely linked together using cryptography. When information needs to be added or updated to the database, the change is verified, authorised, timestamped, recorded and sealed off by private key encryption in a "block" of data, unable to be edited again. The new data block is added to the blockchain by linking it via a cryptographic hash to the previous data block. The updated blockchain is quickly published to, and stored by, all the computing nodes of the network. The database may thus serve as a complete, chronological record of all digital transactions – a secure public ledger identically maintained by each computing node in the network.

Because of data distribution and encryption, digital transactions entered on this ledger are incapable of being retroactively changed. Moreover, private key encryption eliminates the need for a trusted intermediary to prove identity authentication/ownership (ie, you are who you say you are) and the blockchain's protocol authorises a user's permissions (ie, you may do what you are trying to do). Blockchain thus facilitates secure, person-to-person, digital cryptocurrency transactions without the need for a trusted central authority (e.g, a banking system). Software on each computing node can analyse its copy of the ledger to determine whether a particular amount of cryptocurrency has already been spent, necessary to prevent double-spending when there is no such central oversight. Many other applications have been envisioned for blockchain technology, including smart contracts that execute when specified conditions are met, secure identity authentication, peer-to-peer economy/payment systems, stock trading,and logistics.

As with any new computer-based technology, patentability issues may arise, including concerns relating to patent eligibility and adequacy of supporting disclosure.

Section 101

It is crucial that the claims of a patent on blockchain cover one or more *bona fide* improvements to computer technology, and not merely an abstract idea for doing business, otherwise they may violate 35 USC § 101 and be ineligible for patent protection.[3] One way to respond to a Section 101 rejection is to argue that the claims "improve the functioning of the computer itself."[4] For example, one might argue that a proposed blockchain patent claim is directed to an improvement in decentralised computing, data incorruptibility, transparency and redundancy, or secure identity authentication.

Although previously known technologies such as private key encryption, distributed peer-to-peer computing, and incentivising protocols may be referenced, their integration into a new blockchain claim can arguably "improve[s] an existing technological process"[5] for example by eliminating the need for a trusted intermediary to facilitate person-to-person digital transactions or by providing a robust computer network without single-person control. It is thus important that proposed patent claims reflect one or more technological improvements, to ensure they amount to more than merely inputting an algorithm, abstract idea or well-known business method on a computer.[6] Such claims will also be more likely to be patentable in Europe, where a computer-implemented invention must solve a technical problem in a novel and non-obvious manner, rather than merely be directed to a computer program.[7]

Section 112

New technology often necessitates new terminology – the terms "blockchain" and "bitcoin" did not exist until 2008.[8] When needed,

the patent specification should adequately describe or define new terminology in order to ensure compliance with the written description and definiteness requirements of 35 USC § 112. In addition, to comply with the enablement requirement of 35 USC §112, the patent specification must teach those skilled in the art how to make and use the blockchain-related inventions. Practically speaking, the invention should be described in plain English, and if possible should describe the full range of contemplated use cases. This is particularly important to ensure adequate scope of coverage.

A check of USPTO records confirms that the above patentability issues often crop up during prosecution of applications for blockchain. In fact, six out of the 14 US patents that have been issued to date with the word "blockchain" in their title were initially rejected by the Patent Office under Section 101, and four of them were initially rejected under Section 112. Those applicants were able to overcome these rejections.

Blockchain uses a database distributed across numerous computing nodes of a public or private network. Depending on how the blockchain invention is claimed, the distributed computing and user environment may create challenges to proving infringement.

Divided infringement of method claims

Inventions directed to blockchain technology are often expressed as method claims, but blockchains are intended for use by multiple parties. This leads to potential divided infringement issues. Infringement of a method claim is said to be divided when one or more of the individual steps are performed by different parties.[9] Direct infringement may only be found where all of the required steps are either performed by or attributable to a single entity. While courts have recognised that the acts of one party may be attributable to another in certain circumstances, where possible, practitioners should craft method claims to focus on steps that are expected to be performed by the same party and to pursue system or other non-method claims where possible. The patent application should also include claims separately directed to the activities of different entities or components, for example, from the perspective of each transacting party or computing node, as opposed to the whole of the network. If necessary, relationships to other parties or components of the blockchain may be referenced passively, rather than as affirmative elements of the claim.

By whom will system claims be practiced?

By its nature, a blockchain is distributed across a network of nodes, some of which may be controlled or used by different parties. This could lead to disputes about who is using or controlling the claimed "system"? In *Centillion Data Sys v Qwest Comm'ns Int'l,* 631 F.3d 1279, 1285 (Fed Cir 2011), the Federal Circuit held that an infringing use of a patented system occurs when a party "controls the system as a whole and obtains benefit from it." In view of the distributed nature of blockchain systems and depending on the nature of the claims, it could be difficult to show under this legal standard that one party controls the invention as a whole and benefits from it. Practitioners should keep these issues in mind when crafting claims to blockchain systems.

The distributed network of blockchain computing nodes raises the possibility that a portion of the claimed invention may be located or performed abroad. In *NTP, Inc v Research in Motion, Ltd*, 418 F.3d 1282, 1289-90 (Fed Cir 2005), the Federal Circuit ruled that when two domestic users communicate via their BlackBerry devices, it occurs within the US and is an infringement of the system claims, even though a message relay was located in Canada and the messages were transmitted at some point outside of the US. The location of customers and their purchase of the devices established in that case that control and beneficial use of the BlackBerry system occurred within the US.[10] However, the corresponding method claims were not found infringed, because each step was not performed within the US.[11] If possible, practitioners should include claims directed to parts of a blockchain system or process that are likely to be implemented in the same jurisdiction.

Standardisation

To maximise the benefits of blockchain technology, it is important to enable different kinds of blockchain systems. This is a challenge as many blockchain systems have been developed as technological silos. One of the principal obstacles to the widespread adoption, integration and growth of blockchain technology is the absence of any commonly accepted blockchain standards around and upon which developers can build. This may change over time.

Various standards-setting organisations and consortia are working on these issues. For example, the International Organization for Standardization (ISO) has created a technical committee (TC 307) to develop standards for these technologies. Standards Australia, which is the secretariat for TC 307, released a Roadmap for Blockchain Standards in March 2017.[12] Other regional, national and international bodies, have also started standards development work.

As technical standards for blockchain technology emerge, so will opportunities to patent essential aspects of those standards. Whether they choose to participate in standard setting bodies or not, blockchain developers should keep informed of standardisation efforts and adjust their patent portfolio development efforts accordingly.

Footnotes

1. A Kramer, 'More States Eye Blockchain for Records, Businesses', *Bloomberg Law,* 22 February 2018.
2. D Tapscott and R Kirkland, 'How Blockchains Could Change The World', McKinsey & Co, May 2016.
3. *Enfish, LLC v Microsoft Corp*, 822 F.3d 1327, 1336 (Fed Cir 2016); *Finjan, Inc v Blue Coat Systems, Inc*, 2018 WL 341882 at *4 (Fed Cir 10 Jan 2018).
4. *Alice Corp Pty Ltd v CLS Bank Int'l*, 134 S Ct 2347, 2359 (2014).
5. (Id at 2358.)
6. Id at 2360.
7. European Patent Convention, Article 52(2)(c) and (3).
8. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org/bitcoin.pdf (October 2008).
9. *Akamai Techs, Inc v Limelight Networks, Inc,* 797 F.3d 1020, 1023 (Fed Cir 2015).
10. *NTP, Inc v Research in Motion, Ltd*, 418 F.3d 1282, 1289-90 (Fed Cir 2005).
11. Id at 1318.
12. *Roadmap for Blockchain Standards: Report* – March 2017, https://www.standards.org.au/getmedia/ad5d74db-8da9-4685-b171-90142ee0a2e1/Roadmap_for_Blockchain_Standards_report.pdf.aspx

Authors

John Carlin (left) is a partner at Fitzpatrick, Cella, Harper & Scinto. He chairs the firm's financial services Industry practice group.

Douglas Sharrott (right) is a partner at Fitzpatrick, Cella, Harper & Scinto. He chairs the firm's telecommunications and networks industry group.