Blockchain: What is it and can I protect it via patents?

July 31, 2018

By: Josephine Chang

What is Blockchain?

Blockchain technology, some might argue, is the most important technological innovation since the Internet. Those impacted by this technology are not only companies, but also everyday people. Thus, everyone should try to have a basic understanding of what blockchain is, and how one might benefit from it.

The inventor of the blockchain technology is a person or group of people known by the pseudonym, Satoshi Nakamoto. Blockchain was originally devised for cryptocurrency (e.g. bitcoins), but is now evolving into other areas including real estate, health care, insurance, and more.

In simple terms, blockchain is a distributed database containing a list of transactions, also referred to as a distributed ledger. The list of transactions is unique to a particular individual. Information about the transactions is maintained in blocks that are chained together in sequential order, thereby creating a blockchain for those transactions. Once created, the blockchains are stored in millions of computing nodes networked to each other in a peer-to-peer network. This differs from ledgers that are maintained by banks in a central database. The lack of a central database for blockchain technology means no single point of failure, and no single place where hackers can access it to corrupt the database. This allows blockchains to remain secure.

Each computer in the peer-to-peer network maintains a copy of an entire blockchain. The information stored in each block of the blockchain may include details about a transaction, such as data on the sender, receiver, and amount of coins transferred. When a new transaction occurs, a new block is created. New blocks are created by people referred to as “miners” who receive an economic incentive to create the new blocks. Once created, a new block is sent to all the nodes in the network for verification that the block has not been tampered with. If verification is successful, each node adds the new block to its copy of the blockchain. Once added, the block cannot be removed making blockchains irreversible.

In addition to information about a particular transaction, each block stores three other sets of information: 1) a hash of the block; 2) a hash of the previous block; and 3) proof of work. A hash is a value that identifies the block and the contents of that block. Much like a fingerprint, the hash value is unique to the block. If the contents of the block changes, so does the hash value. Hash values, therefore, help detect any attempt by hackers to make changes to the block.

Another piece of data that is stored in each block of the blockchain is the hash of the previous block. The fact that each block must not only store its own hash but the hash of the previous block, is effectively what creates the chain of blocks. This is also a major reason why blockchains are secure. If a hacker does tamper with one block, causing a new hash to be created, the hash of all following blocks in the chain must also be recomputed in order for those blocks to be valid.

The last piece of data stored in a block, the proof of work, is a mechanism that slows down the creation of new blocks. It is a mechanism utilized by the miners to verify that transactions within each block are

legitimate. In order to do so, miners solve a puzzle known as a proof-of-work problem. A reward is given to the first miner that solves each block's problem, thereby verifying that the block is legitimate.

As an example of how blockchains might be created and used, let's assume that there are three people who want to move money from one to another. At the inception of the network, A has 10 coins. Thus, the first block of the blockchain contains this information: A = 10 as well as a hash value for the block. Now, A wants to move 5 coins to B. Because A has 10 coins, the transaction is valid. Thus, a second block is created for the new transaction, and the second block is linked to the first block by not only storing the hash value of its own block, but the hash value of the previous block.

Now, let's say that B wants to move 15 coins to A. This transaction is not valid since B does not have 15 coins.Thus, the new transaction is not verified, and is not added to the blockchain.

Patent Protection for Innovotions Relating to Blockchain

The increasing popularity of blockchain technology has also increased the number of patent applications for innovations related to this technology. So far, over 740 blockchain patent applications have published worldwide, a dramatic increase since 2016.

Although many applications have been filed for blockchain-related innovations, getting a patent in this area may be far from smooth sailing, especially in light of the 2014 Supreme Court decision in *Alice Corp. v. CLS Bank Int'l,* 134 S. Ct. 2347 (2014). The court in *Alice* held that claims directed to mitigating "settlement risk" (i.e. risk that only one party to an agreed-upon financial exchange will satisfy its obligation) was a patent-ineligible abstract idea under Section 101 of the Patent Act. In a similar manner, a patent examiner might conclude that innovations surrounding blockchains are patent-ineligible abstract ideas. Such rejections might have merit under the current state of the law if the invention utilizing blockchain technology merely seeks to protect a fundamental economic practice, protect a method of managing relationships or transactions between people, or is merely directed to organizing or analyzing information in a way that could all be performed mentally.

Knowing that potential hurdles might exist under Section 101 of the Patent Act should prompt patent applicants to draft their patent applications in a manner that maximizes the chances of overcoming or avoiding a rejection under this section. In doing so, applicants may turn to guidance provided by the courts and by the Patent Office itself. For example, both the Patent Office and the Federal Circuit have acknowledged that innovations that are aimed at bringing technical improvements are patent-eligible. The technical improvements may be the functioning of the computer itself, or improvements to another technology or technical field.

One useful case to consider is *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC,* 827 F.3d 1341 (2016). The claims at issue in that case were directed to a system and method for filtering Internet content. The Federal Circuit agreed that filtering content is an abstract idea because it is a long-standing, well-known method of organizing human behavior. The Federal Circuit also agreed that the limitations of the claims, taken individually, recited generic computer, network, and internet components, none of which was inventive by itself. However, the Federal Circuit concluded that the combination of the claimed elements amounted to significantly more than the abstract idea because of the non-conventional and non-generic arrangement of those elements that provided a technical improvement in the art. *BASCOM Global Internet Servs. v. AT&T Mobility LLC,* 827 F.3d 1341, 1350-51 (2016).

Another case to consider is *DDR Holdings, LLC v. Hotels.com, L.P.,* 773 F.3d 1245, 1258-59, 113 USPQ2d 1097, 1106-07 (Fed. Cir. 2014). The invention that was patented in that case addressed a

business challenge (retaining website visitors), which was particular to the internet. The court found that the claimed invention differed from other claims found by courts to recite abstract ideas because the claimed invention did not "merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet." *(Id at 1257.)* Instead, the claimed solution was "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer network." *(Id.)*

As in *Bascom* and *DDR*, if a blockchain-related invention provides a technical improvement to a technical problem, such an invention should be deemed to be patent eligible. For example, the invention might provide a solution to a technical problem or a deficiency introduced to the computing system due to the use of blockchain technology. If the solution provides improvements to the functioning of the computing system itself, such an invention should be deemed to be patent eligible. The technical solution, however, should be described with particularity in the patent application. The more general the description of the solution/invention, the higher the likelihood that it may be deemed to be an abstract idea.

The technical solution provided by the invention need not, however, necessarily be one that improves the functioning of a computer itself in order to be patent-eligible. The solution might be one that provides improvements to some other technology or technical field. For example, if a blockchain-related invention does not improve the functioning of the computer itself, but rather, brings improvements to technologies such as encoding/decoding technologies, error correction technologies, digital transmission/download technologies, data compression technologies, or technologies integral to the internet, then the invention should not be deemed to be merely a patent ineligible abstract idea.

In summary, blockchain technology has opened the door to a new way of engaging in transactions that might be deemed to be revolutionary by many. Further innovations surrounding this technology are anticipated, and patent applications might be desired for many of those innovations. Under the current state of the law, however, there might be obstacles in obtaining patents for those innovations. Understanding what the obstacles might be, and carefully crafting patent applications to increase the likelihood of overcoming such obstacles, will allow applicants to maximize their chances of obtaining patents for their inventions.