

## **Blockchain What is it and what are its IP issues?**

Yuhon Tom Zhang  
**ROBIC, LLP**

Lawyer and Patent Agent in Canada and the United States

When we think about systems for computing large amounts of data, we usually think about server farms formed of numerous computer mainframes running together in air conditioned facilities. Distributed computing sits at the opposite of the spectrum - data is processed in a disparate manner across loosely connected networks of computers. A particularly interesting application of distributed computing is with “blockchains”.

A blockchain is a type of database stored on many computers in a peer-to-peer network, and is particularly adapted for recording transactions. Transactions are recorded within “blocks” which are stored on each computer in the network. As new blocks are added, they are linked to all preceding transactions, thereby forming a chain of blocks. New transactions must be validated by all computers in the network by checking the new transaction against all earlier transactions. Since each computer in the network has its own copy of the blockchain, the data is seen as being more secure than traditional methods in which data is stored in a single central location.

### **Blockchain for cryptocurrency**

Blockchain is best known for being the technology that underpins Bitcoin and other similar types of cryptocurrency. Transactions of Bitcoins are recorded in blockchain transaction ledgers. The owner of a given Bitcoin stores the digital credentials to his or her bitcoin holdings in a digital wallet. The digital credentials are used to validate ownership by verifying the blockchain ledger. For example, if Party A transfers a Bitcoin to Party B, Party A provides his or her credentials and the blockchain ledger is checked to determine that Party A is the rightful owner of that Bitcoin. The blockchain is then updated accordingly to indicate that Party B has become the new owner of the transferred Bitcoin.

Entries in the blockchain ledger are secured using cryptography, hence the term “cryptocurrency”. The peers in the network verify the blockchain ledger by deciphering these encrypted entries. New units of the cryptocurrency are awarded to those peers that connect their computers to the network to participate in the validation and verification of transactions.

Currently, it is possible to buy various goods or services online with various types of cryptocurrency. One type of digital currency can also be exchanged for other types of digital currencies, or even for real currencies.

### **Beyond cryptocurrency**

Given the potential of blockchain technology to leverage distributed computing power, many people have started envisioning uses for the blockchain in applications beyond cryptocurrency. These additional applications have generally been known as Blockchain 2.0. One area of interest is smart contracts. In a smart contract, the terms of the contracts can be set out in computer code. When two parties to a contract execute their respective obligations of the contract, a smart software program can verify and enforce that contract. The smart contract itself, the execution of the contract and the verification can be stored in the blockchain.

Smart contracts are particularly well-adapted to online interactions. The smart contract can define the actions by online parties (ex: a user listening to a song from a streaming service) that will trigger a payment (ex: a royalty is paid to the author/publisher of the song).

Presently, smart contracts are seen as being useful for enabling decentralized micropayments, such as paying a very small fee (ex: a few cents) in return to accessing small bits of digital content (ex: paying to read a news article or to listen to the song). In the future, it is possible to envision smart contracts playing an important part in a world that becomes increasingly automated.

Given the vast potential, it is not surprising that tech start-ups have sprung up to provide innovative ways of offering services leveraging blockchain technology. At the same time, large financial companies have also begun research and development activities in this space. In order to claim a piece of the space for themselves and to not be left behind, companies have also begun filing patent applications for the new blockchain technologies that they have developed.

### **Is blockchain technology patentable?**

There is an ongoing debate in many countries regarding whether computer-implemented inventions are eligible for patent protection.

In the U.S., the courts have rejected a blanket ban on software inventions, but have stated that inventions directed to abstract ideas, such as fundamental economic practices and methods of organizing human behaviour, are not patentable.

In Canada, the Federal Court of Appeal stated in its 2011 Amazon One-Click decision that an invention must not have a disembodied idea, must have a practical application, and must have a commercially useful result. Again, there is not an outright ban on software inventions under Canadian law.

In Europe, while software is not patentable per se, such prohibition does not apply for inventions for entire computer systems.

Whether a particular Blockchain invention will be eligible for patenting in a given jurisdiction will depend on the particular nature of that invention. Given that the core of blockchain is technological in nature (defining specific data structures, algorithms and network configurations), it is likely that these core innovations will be eligible for patent protection in many countries. Innovations that apply blockchain technology in a novel way to change current financial practices will also likely be patent-eligible. However, simply applying generic blockchain technology to known financial practices will likely be harder to protect.

### **Patent protection and future innovation**

Some pessimists see patents as roadblocks for future innovation. As individual companies carve out small areas of blockchain space for themselves, others can be prevented from operating and innovating in those spaces.

Another possible outcome is blockchain technologies converging towards a common set of standard practices and technological norms as the technology matures. Standardization seems likely considering that legal and regulatory schemes will certainly be developed. Consequently, a set of standard-essential patents may also emerge, in which companies wishing to operate in the space will be required to obtain licenses to such patents. This scenario is similar to the telecommunications industry.

A rise in patent trolling activities is also foreseeable. That is, companies that hold patents for blockchain technology but do not actually operate in the space will attempt to monetize their patents by suing and/or seeking licensing fees from other companies that do operate in the space. However, if patent offices continue to examine patent applications in a strict manner and do not allow overly broad patents, the level of patent trolling activities may be lower than what is currently being seen.

### **Blockchain, patents and open source**

A fundamental philosophical contradiction exists between the open source software technology and patenting. Whereas open source is based on the philosophy that all innovation should be free to be used by all, patenting seeks to prevent all others from using the patented innovation. Large amounts of open source software are licensed under terms that oblige the licensee to also make the software available for others to use. The courts have yet to provide an answer to the question of how such open source licenses impact patents that cover innovations developed using open source software.

A large part of blockchain technologies are being developed using open source software. For example, the software enabling Bitcoin is open source. It will be interesting to see if the patenting vs open source dichotomy becomes an important issue as the industry matures.

---

**Conclusion**

It would not be surprising for blockchains to quickly change how financial transactions are carried out over the Internet. It will be interesting to see whether legal frameworks, such as IP, can keep pace with such changes.