MASSACHUSETTS LAWYERS WEEKLY

A primer on blockchain and cryptocurrencies

By: Gregory Gerstenzang June 7, 2018

Intellectual property attorneys should familiarize themselves with blockchain technology to better assist internal and external clients in identifying potential opportunities to enhance business operations utilizing the technology and to develop a strategy to protect IP associated with any such business enhancements.

Blockchain technology has grown in popularity and, subsequently, the number of patent filings associated with it has recently skyrocketed. The Bitcoin cryptocurrency meteoric rise and fall in value contributed to bringing this technology into the public eye.

Although many have heard of Bitcoin, questions still surround blockchain and its uses. The following facts and observations may help provide some clarity to this subject.

About blockchain

Blockchain is an unalterable distributed ledger, or records, of transactions between parties without being maintained by a centralized intermediary or authority.

A blockchain includes data blocks within a certain range of sizes, with each recording a number of different transactions. As transactions are performed, records are gathered together to form a new block, which is appended to the end of existing blocks in the blockchain.

Blockchain data is then used to obtain verification of a performed transaction and ownership of assets associated with it.

Blockchain and cryptocurrencies

Blockchain was invented in 2008 by Satoshi Nakamoto (a pseudonym) for use as a transaction ledger for Bitcoin, arguably the first publicly known application utilizing blockchain technology.

Bitcoin can be traded on a peer-to-peer basis between users who do not need to share their true identities, and thus has been categorized as a "cryptocurrency."

Bitcoin, however, is only one currency application utilizing blockchain technology. Others include the Ether cryptocurrency associated with the Ethereum platform, Litecoin, XPR and Dogecoin cryptocurrencies.

The types of transactions that can be recorded in a blockchain are not limited to financial matters or cryptocurrencies. Additional applications of blockchain technology will be discussed below.

Secure record management

Each block in a blockchain is secured and linked using a cryptographically generated code, referred to as a cryptographic hash, of the immediately previous block.

The cryptographic hash is generated from a combination of data associated with the transactions records in the block and the cryptographic hash of the preceding block.

An attempt by a hacker to alter a transaction record in a block will result in a change in the cryptographic hash. That change will propagate changes in the cryptographic hashes in all subsequent blocks in the blockchain, rendering the alteration in the transaction data readily apparent.

Blockchain maintenance

As noted above, there is typically no centralized intermediary or authority that maintains a blockchain ledger. Instead, copies are maintained by the numerous users of the blockchain, often at their own local servers.

The integrity is preserved by the users comparing their ledgers against each other to check whether any individual ledger has been compromised; for example, by a hacker attempting to alter a previous transaction record.

If a discrepancy is detected, a majority rule system is typically employed in which a ledger that does not match the majority of users is considered corrupted and may be replaced by a copy of the ledger that is agreed upon by the majority as being correct.

A hacker attempting to alter a record would thus have to alter the ledgers of more than half of all the users of a blockchain. That would have to happen when new blocks are added to successfully alter the distributed ledger, which would be incredibly difficult to do.

Because of that, neither the Bitcoin nor Ethereum ledgers are believed to have ever been successfully hacked.

Management of addition of new transactions

As new transactions in a blockchain are completed, records of it are sent to the users. When a sufficient number has been performed, miners (individual users) attempt to be the first to complete the cryptographic operations on the new transactions to create a cryptographic hash for the new block to append to the existing blocks of the blockchain.

The first miner to successfully generate the cryptographic hash for the new block is awarded with an incentive; for example, in the Bitcoin system, a number of newly minted Bitcoin.

The generation of a cryptographic hash for a new block involves combining the cryptographic hash of a previous block with the record of transactions in the nascent block that satisfies a set of rules — for example, a specific length (e.g., 64 bytes) and a specific limit on complexity.

According to the rules established for a blockchain, the generation of a cryptographic hash for a new block may require a large amount of computational power, utilizing a brute force methodology to "solve" the cryptographic problem associated with generating the new hash.

In the Bitcoin system, for instance, even when using high-powered computing systems, it can take 10 minutes to generate a compliant cryptographic hash for a new block having a size of about 1.5 megabytes.

> *Blockchains can be used to create records of land registration and to record title in any property — such as automobiles, high-value art, collectibles, ownership in businesses, or assignments of rights to intellectual property.*

Other uses of blockchain technology

Blockchains can be used to generate permanent records of nearly any type of transaction. For example, they have created records of land registration and can be used to record title in any property, such as automobiles, high-value art, collectibles, ownership in businesses, or assignments of rights to intellectual property.

Blockchains can also be utilized in supply chain management to track and record the handoff of high-value assets to different carriers along the supply chain.

In the area of copyright, a user can upload a copy of a copyrightable work to a blockchain to produce a permanent record of the date of creation and ownership of the work. As one example, Eastman Kodak announced plans to develop a blockchain platform that allows users to record their digital photographs and to facilitate licensing of the same nature.

Similarly, to copyright, services exist for an inventor to submit evidence of a new invention to a blockchain, establishing a record of date of conception and ownership of the intellectual property associated with the invention.

Additionally, blockchain-based exchanges can be utilized for peer-to-peer trading of securities or commodities, similar to how Bitcoin can be traded, without the need for a broker and associated transaction fees.

Smart contracts

Smart contracts that utilize blockchain technology can be created on the Ethereum platform, among others.

In a smart contract, the terms are permanently recorded in a blockchain. Performance toward satisfaction of the contract terms are added as contractual obligations are completed. Once the contractual obligations of one party to the contract are satisfied, the contract is automatically executed so that the obligations of the other party are fulfilled.

No third party is required to facilitate, verify or enforce performance of a smart contract; thus, these may provide enhanced security, reduced settlement times, and reduced transaction costs as compared to traditional contracts.

Initial coin offerings

Newly formed companies or startups are beginning to obtain financing by initial coin offerings as an alternative, or in addition to, traditional venture capital or angel financing.

In an ICO, which is a type of crowdfunding, a new technology startup can obtain financing by selling its own virtual currency or tokens to investors for Bitcoin or Ether.

The startup's investors can use the virtual currency to pay for services to be provided by the new company once it becomes operational. Some investors may purchase the virtual currency of the startup in hopes that the value of the currency will increase over time. Therefore, a new company can often obtain significantly more capital from an ICO than through traditional venture capital.

However, and as opposed to venture capital financing, an ICO does not give equity in the newly formed company to the investors. It is also important to note that virtual currencies sold via ICOs may not need to comply with regulations established by the Securities and Exchange Commission such as for stocks or bonds.

Well over $3 billion was raised by startup companies via ICOs in 2017.

IP trends

Patent filings associated with blockchain technology have been increasing exponentially over the last five years.

As of early April 2018, there were close to 500 patent applications filed in the U.S. Patent and Trademark Office with the terms "blockchain" or "distributed ledger" in their title, abstract or claims. This is in comparison to just over 100 in 2013. At least 40 of the applications have been granted patents as of early April.

Players in blockchain patent filings

The majority of patent filings has been from blockchain-specific companies, such as startup cryptocurrency exchanges, as well as traditional financial firms.

As of January 2018 in the U.S., Bank of America had the greatest number of granted blockchain patents, with IBM and Mastercard in second and third place, respectively.

Additionally, more than half of the blockchain-related patents filed in the U.S. in 2017 were from Chinese companies such as nChain.

Attorneys should be educated on the nature of IP associated with blockchain technology for which potential or actual competitors of their clients have sought protection. That way they can help guide their clients toward implementations of this technology that do not run afoul of competitors’ intellectual property.

Gregory Gerstenzang is an intellectual property attorney at Lando & Anastasi in Cambridge. He can be contacted at GGerstenzang@LaLaw.com.