HOW BITCOIN WORKS:
A TECHNOLOGICAL DESCRIPTION OF BLOCKCHAIN-BASED CRYPTOCURRENCIES FOR NON-TECHNICAL LAWYERS

by JOSEPH W. GUZZETTA

It is no secret that blockchain-based currencies are enjoying a boom, both in economic and legal terms. Bitcoin, the undisputed king of blockchain-based currencies, recently shot past $4,000 in August 2017. While in its infancy, regulation of virtual currencies is increasingly becoming a focus of agencies such as FinCEN, the SEC, and other regulators. Any attorney hoping to counsel clients on the emerging legal trends relating to blockchain-based currencies would be at a distinct disadvantage without a basic understanding of how Bitcoin and the blockchain works.

> The blockchain is a public ledger, to which anyone can make edits, that records every Bitcoin transaction since the inception of the cryptocurrency.

The purpose of this article is to provide attorneys with a general technological overview of how blockchain-based technology works, what a block is, and how blocks are added to the blockchain in a way that cannot later be altered. This summary necessarily simplifies a very complex technology in terms that I hope are understandable to anyone with or without a technological background.

Bitcoin Basics

This article will focus on Bitcoin, but the principles discussed apply to any blockchain-based currency (such as Litecoin, Darkcoin, etc.). Bitcoin is a virtual cryptocurrency, meaning it exists wholly electronically and utilizes cryptography in order to secure transactions. Bitcoin was developed in 2009 by Satoshi Nakamoto (a pseudonym), and was designed to overcome many of the problems that had plagued—and in many cases led to the downfall of—virtual currencies that had existed up until that time, including centralization and vulnerability to government regulation.

Bitcoin are held in "wallets." A "wallet" is nothing but a pair of very long numbers and letters—a "public key" and a "private key." In order to transfer Bitcoin to another user, the sender instructs his Bitcoin software to send Bitcoin to the recipient's public key. The recipient can only access and spend those Bitcoin, however, by utilizing the private key. In a sense, the public key tells senders the address of the wallet so that deposits (but not withdrawals) can be made to the wallet, and the private key unlocks the Bitcoin wallet so that Bitcoin can be withdrawn from it. Bitcoin wallets are nothing but mathematical addresses; they have no physical form. Private keys must be closely guarded in order to prevent Bitcoin theft (some of the largest Bitcoin thefts—including the highly-publicized MtGOX collapse—resulted from lack of adequate security relating to wallet private keys).

Bitcoin transactions are recorded publicly in the "blockchain." The blockchain is a public ledger, to which anyone can make edits, that records every Bitcoin transaction since the inception of the cryptocurrency. When a user downloads the Bitcoin software, which allows him to make Bitcoin transactions, his or her computer makes a copy of the blockchain and stores and updates it on the user's computer. Because anyone can make changes to the blockchain, any number of different versions of the blockchain can exist at any one time. Bitcoin users—particularly "miners" who attempt to add blocks to the blockchain in exchange for the corresponding reward—"vote" on which blockchain is the valid one by adding blocks to that blockchain, hence making it longer than the others. In other words, the valid blockchain is generally the one that is the longest.

Hashing Functions

Understanding how blockchain-based currencies work starts with understanding hashing. A hashing function is a mathematical function that has the following properties (among others): (1) it is capable of taking an

input of any size; (2) it yields an output of a fixed size no matter the size of the input; (3) it minimizes "hash collisions," or instances when two different inputs yield the same output; (4) it yields outputs that cannot be used to determine the input; and (5) a small change in input will result in a drastic change in output.

Great effort is put into developing secure hashing functions. One of the most popular hashing functions used in cryptography today is called Secure Hash Algorithm 256, or "SHA-256" (pronounced "shah-two-fifty-six"). Developed in 2012 by the National Security Agency, SHA-256 is the hashing function that powers Bitcoin. As an example, hashing my name, "Joe," through the SHA-256 algorithm yields a long hexadecimal number:

2ac4aef4b9914868b4a2a0fe4734c64f2855d81c257e0d46c0dc6533ca69f63f

But hashing my name with a lower case "j" yields a completely different result:

e78c1300cce6b69a800cb5d34aed3e2cb52bd5662fabe77c83748d9aa02caea8

While it is easy to take the input and derive the output (as I just did above), it is thought to be very difficult or impossible to derive the input knowing only the output.

The Leading Zero Problem

Now, suppose I posed a problem: hash my name ("Joe"), but append to it a random number such that the hash result starts with the number zero. I can solve this problem by simply hashing over and over again ("Joe1," "Joe2," "Joe3," etc.) until the result starts with zero. It is painstaking, but doable. Hashing my name with "12" appended to it ("Joe12") yields:

029dc2070df1aa8f2567acbc58e8ac5cb1f461b0701f777ec560811e6f07859c

I can adjust the difficulty of this problem (and hence the average time it takes to solve the problem) by requiring fewer or more leading zeros. For example, it takes considerably more time to find a result that begins with two leading zeros: I had to hash from "Joe1" to "Joe895" (which took me well over an hour) before I found that the SHA-256 hash for "Joe895" is:

00b077009ca22b6c7bd38ff3cb4f98f7f7186424b3e15cd48ff24abd9f947b75

If I wanted to find a number that caused the hash of my name to start with three leading zeros, it would take even more time and computing resources.

The Blockchain

The blockchain is, not surprisingly, a series of blocks. A block is a collection of Bitcoin transactions. When one person transfers Bitcoin from one wallet to another, that person's Bitcoin software broadcasts the transaction (for example, "Send 10 Bitcoin from Wallet X to Wallet Y") to all Bitcoin users who are running the Bitcoin software.

Bitcoin miners collect these transactions into a "block." They add to their block three things: the reward transaction (transferring 12.5 newly-created Bitcoin to a wallet of their choosing), the hash of the prior block, and something called a "nonce" (or a "number only used once"). Miners then hash the block they create, and determine whether or not the result contains the requisite number of leading zeros—currently approximately 17. (This number is set such that it takes the total computing power of all Bitcoin miners 10 minutes, on average, to solve a block.) If the resulting hash does not contain the requisite number of leading zeros, the miner adjusts the nonce and tries again.

ON TOPIC

Because anyone can make changes to the blockchain, any number of different versions of the blockchain can exist at any one time.

If the hash does contain the requisite number of leading zeros, the block is "solved," and the miner broadcasts that solution to other miners. Those miners check the validity of the block and, if they agree that the block is valid, they will "vote" on the validity by adding it to their version of the blockchain, and beginning to work on attempting to solve the next block.

Why go through all of this trouble to solve a block? Reward. Bitcoin miners are currently rewarded with 12.5 Bitcoin for adding a block to the blockchain. The first transaction in each new block is a reward transaction where the miner gives 12.5 Bitcoin to him or herself. Because a small change in input will result in a drastically different hash, this means that each Bitcoin miner will be searching for a different nonce that solves the current block. If the miner solves the block before anyone else, his block—giving 12.5 Bitcoin to himself—is added to the blockchain to the exclusion of others'.

With the current price of Bitcoin hovering around $4,000 each (making each solved block worth approximately $50,000), it is not difficult to see why people would want to invest in expensive and sophisticated equipment dedicated to Bitcoin mining. These mining chips—which are often linked together into mining "farms"—basically do one thing and one thing only: hash very, very fast. The reward is set to halve every 210,000 blocks added to the blockchain until, in approximately 2140, it will be reduced to zero and Bitcoin miners will rely on transaction fees only to be paid for their hashing work.

One additional item of note regarding blocks: recall that each miner adds the hash of the prior block to the next block. It is this item that links the blocks in a chain. By adding the hash of the prior block into the current block, the blockchain becomes locked down in such a way that changes (for example, suppose I went back to the very beginning of the blockchain and gave myself 100,000 Bitcoin) reverberate throughout the blockchain in an obvious way. If I made that change to the first block, the next block would no longer hash to the requisite number of leading zeros because the hash of the prior block changed. Every block down the chain would no longer be validly solved, making my malicious change highly obvious and, without certain very unlikely conditions, impossible.

Conclusion

This description is necessarily simplified from reality. However, it should provide an understanding of how the blockchain functions sufficient for attorneys practicing law in this emerging area. Satoshi Nakamoto's invention was an extremely clever way to secure a cryptocurrency. These same features also make blockchain-based technology, by nature, resistant to government regulation. As regulators grapple with how to regulate the unregulatable, attorneys who have a basic understanding of how this technology works will be at an advantage.

Joseph W. Guzzetta *is a trial lawyer who practices at Severson & Werson, P.C. His interests include privacy law and the regulation of cryptocurrencies and other emerging technologies. He can be reached at jwg@severson.com.*

This article first appeared in Orange County Lawyer*, October 2017 (Vol. 59 No. 10), p. 34. The views expressed herein are those of the author. They do not necessarily represent the views of* Orange County Lawyer *magazine, the Orange County Bar Association, the Orange County Bar Association Charitable Fund, or their staffs, contributors, or advertisers. All legal and other issues must be independently researched.*