New York Law Journal

White-Collar Crime

WWW.NYLJ.COM

An ALM Publication

VOLUME 257—NO. 62

MONDAY, APRIL 3, 2017

The Promise of **Blockchain Technology** To Combat **Money Laundering**

BY CHRISTIAN EVERDELL
AND DANIEL MANDELL

SHUTTERSTOCK

If you have been following the news recently, you probably know what Bitcoin is. It is a digital currency or cryptocurrency—or to use the language of Bitcoin's enigmatic creator, Satoshi Nakamoto, a "peer-to-peer electronic cash system"—that was first introduced to the world in 2008.

You probably also know that Bitcoin has had a somewhat checkered past. For example, Bitcoin was the only form of payment accepted by Silk Road, the online drug bazaar that was shut down in 2013, and is frequently the cryptocurrency of choice for ransomware hackers who demand Bitcoins in exchange for unfreezing your computer files.

Despite the ubiquitous familiarity of Bitcoin, a much smaller number know what the blockchain is. On a practical level, the blockchain is the digital ledger system that keeps track of, and securely records, all Bitcoin transactions that have ever occurred from day one to the present. On a loftier level, it is what creates trust and confidence in the validity of Bitcoin transactions, which allows the system to function. Quite simply, without the blockchain, there is no Bitcoin.

But recently the blockchain has moved out of the shadow of Bitcoin and has emerged as a potentially groundbreaking technological innovation that many are convinced will have countless transformative beneficial applications. One of the most touted applications is in the area of bank transfers and anti-money laundering (AML). Paradoxically, the same technology that made Bitcoin so attractive to criminals as a way to move their money may now help financial institutions crack down on illicit transfers. So how can the blockchain help combat money laundering?

How Does Blockchain Work?

To appreciate how blockchain technology might be applied in the AML context, it is useful to understand first how it functions in its native environment of Bitcoin transactions and how Bitcoin transactions differ from typical bank transactions.

Let's look at a relatively simple bank transaction between Anna and Ben, where Anna and Ben have accounts at the same bank. Anna owes Ben $10 and tells her bank to transfer $10 from her account to Ben's account. The bank

CHRISTIAN EVERDELL *is counsel and* DANIEL MANDELL *is an associate at Cohen & Gresser.*

debits Anna's account by $10 and credits Ben's account by $10. No money actually moves anywhere—the transaction is simply reflected as a corresponding debit and credit that balance out in the bank's electronic ledger system.

In this example, the bank is the trusted intermediary between Anna and Ben that handles all of the accounting and ensures that the transaction is carried out properly. Anna trusts the bank to credit the correct bank account (Ben's) with the correct amount ($10). Ben trusts the bank to verify that Anna has at least $10 in her account to cover the transaction before the transaction settles. And both Anna and Ben trust the bank to maintain an accurate ledger of their accounts so that when they check their balances, they have confidence that the amounts reflected are correct.

> The blockchain has moved out of the shadow of Bitcoin and has emerged as a potentially groundbreaking **technological innovation** that many are convinced will have countless **transformative beneficial applications.**

In a Bitcoin transaction, however, there is no trusted third-party intermediary like a bank. Bitcoin was specifically designed to be a decentralized system that eliminates the intermediary and allows Bitcoin users to make transfers directly to and from each other. But without a trusted intermediary to audit and record Bitcoin transactions, how can Bitcoin users keep track of who paid what? And how can they be certain that the system is secure? Answer: the blockchain.

The blockchain is the general ledger for Bitcoin transactions. It contains a complete, unbroken audit trail for every Bitcoin transaction that that has ever taken place. But the blockchain is not maintained by a single central authority like a bank. Instead, it is a distributed ledger that is maintained by thousands of computers around the world, called "nodes," each of which contains a complete copy of the blockchain.

The people who operate the nodes are called "miners." It is the miners' job to update the blockchain as new Bitcoin transactions occur on the Bitcoin network. Miners identify all of the pending transactions on the Bitcoin network for a given time period and then aggregate those transactions into a "block." To create the block, the miners run the transactional data through a series of mathematical calculations to produce a "hash" value—a unique string of numbers and letters that identifies that data—which is then stored on the block. The purpose of the hash value is to ensure that the data in the block can never be altered. If someone were to change the data in the block even slightly, the hash value would change and the block would be recognized as a fake. Once the new block has been successfully created, it is added to the blockchain, which is updated instantaneously across all of the nodes on the network.

To see how this works in practice, let's take our previous example, but now Anna owes Ben 10 Bitcoins instead of $10. How does Anna get those 10 Bitcoins to Ben? First, Anna needs to know Ben's Bitcoin address, which is the rough equivalent of a bank account number for Bitcoins. Next, Anna goes to her computer or smartphone and opens her Bitcoin "wallet," which is a software program that keeps track of her Bitcoins and gives her access to the Bitcoin network to make transfers. Anna sends a request to the network to update the blockchain to reflect a transfer of 10 Bitcoins from her Bitcoin address to Ben's Bitcoin address. The miners see the request and verify that Anna actually has 10 Bitcoins in her Bitcoin address. They then group Anna's transaction with numerous others into a new securely hashed block and add it to the blockchain. Once this process is complete, which usually takes about 10 minutes, the transaction is final and Ben's Bitcoin wallet will show that he has 10 more Bitcoins (and Anna's, 10 less). All of this is done quickly, securely, and without the need of a bank.

Blockchain's Troubled Youth

Despite all the current excitement about the blockchain, it got off to a rocky start. In its infancy, the blockchain was inextricably linked to Bitcoin. And Bitcoin, when it was first introduced in 2008, quickly became a popular method among cyber-savvy criminals to pay for illegal goods and services and to launder their money. The possible alternative applications of blockchain's distributed ledger system were not immediately apparent and would not bubble up to the surface until much later.

It is easy to see why criminals flocked to Bitcoin. First and foremost, it allowed them to remain hidden and transfer funds anonymously. That is a little counterintuitive, because the blockchain is entirely public. Anyone can access the blockchain through their Internet browser and review the transactional data that it contains. The key is that the blockchain, by design, does not record any information about the participants to the transactions themselves.

When Anna sends her 10 Bitcoins to Ben, the only information that is recorded in the blockchain about that transaction are Anna's Bitcoin address, Ben's Bitcoin address, the amount of the transfer, and the date and time the transfer was added to the blockchain. Nothing that might identify Anna and Ben is recorded—no names, no phone numbers or email addresses, not even the IP address that Anna used to access the Bitcoin network to execute the transaction. This makes it virtually impossible for someone—say, a law enforcement officer—to trace the transaction back to Anna and Ben.

It is true that the blockchain captures the Bitcoin addresses of the participants. But these randomly generated strings of letters and numbers are meaningless to the outside observer. They only mean something to Anna and Ben. Anna knows her own Bitcoin address and knows Ben's too, because Ben gave it to her to complete the transaction. Ben knows his own Bitcoin address and can figure out Anna's because he can check the blockchain and see which Bitcoin address sent 10 Bitcoins to his Bitcoin address on the day that Anna said she would make the transfer. But without this type of external information to connect the dots, the blockchain data remains opaque and Anna and Ben stay hidden to the wider world.

The contrast to traditional bank transfers is evident. Banks cannot provide this type of anonymity because banks, as part of their AML controls, have know-your-customer (KYC) requirements. Before a bank can do business with a new customer, they must satisfy themselves that they know who they are dealing with. They require the customer to provide personal information—a name, an address, etc.—and documents to verify identity, like a driver's license. All of this information is then linked to the customer's bank account. It goes without saying that this is exactly the sort of information a criminal actor would rather not have to hand over. And by using Bitcoin, they do not have to.

Even worse for the would-be criminal, banks keep all of this information on file and will readily provide it to law enforcement agencies with a subpoena. Hence, the blockchain's decentralized design offers yet another advantage: There is no central repository of KYC information. The blockchain itself contains only limited information, and law enforcement agencies cannot subpoena the blockchain to obtain more.

A Brighter Future: Blockchain's Potential in AML

If the blockchain's past was murky, its future seems bright indeed. Blockchain evangelists are trumpeting that distributed ledger technologies will revolutionize entire industries, from banking and financial services, to securities, to insurance. Business and venture capitalists have lavished significant attention and money on developing the technology—over $1.4 billion in the past three years alone. The hype around the blockchain has now reached a fever pitch.

In the banking sector, there is a great deal of optimism that distributed ledgers will vastly improve AML compliance. But how can a technology that seems so tailor-made for facilitating money laundering now be the answer to that problem?

The leading solution among the banks has been to develop a private or "permissioned" blockchain, as opposed to an open or "permissionless" blockchain. Instead of allowing anyone to become part of the network, as was the case with the Bitcoin blockchain, only trusted banks are given permission to join the network. The member banks each function as a node in the system and maintain a shared ledger that securely records all of the transactions on the network using the hash value process of the original Bitcoin blockchain. In a private blockchain like this, the ledger is distributed among the member banks, but the system is not decentralized. The banks retain their status as the trusted intermediaries that verify and record the transactions on the network.

Ultimately, of course, **private blockchains will not eliminate the problem of money laundering entirely.** No matter how efficiently member banks obtain and share KYC documentation, sophisticated criminal actors can still provide false information that passes muster.

Private networks such as these are still being tested. But if they are successfully implemented, the potential AML benefits are numerous:

- First, KYC documentation could be incorporated into the private ledger and shared simultaneously with the other member banks, eliminating the need for each bank to perform duplicative KYC due diligence on the same customer.
- Second, if the member banks permit the banking regulators to operate a node on the system, the regulators could receive real-time reports of suspicious activity at a greatly reduced cost to the banks.
- Third, because the private blockchain maintains an unbroken audit trail of every transaction on the network, it will be harder for money launderers to obfuscate their transfers by washing the money through multiple shell accounts. Those transfers could be unwound fairly easily using the information in the blockchain.

Ultimately, of course, private blockchains will not eliminate the problem of money laundering entirely. No matter how efficiently member banks obtain and share KYC documentation, sophisticated criminal actors can still provide false information that passes muster. And money launderers who prefer to avoid the watchful eye of regulated financial institutions entirely will still find a plethora of digital currencies available to them that will transfer their funds completely anonymously. But for those entities who take AML seriously, blockchain technology may prove to be a significant step forward.