Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Applying Blockchain To Commercial Real Estate Transactions

By **Jeffrey A. Lenobel and Aaron C. Retter, Schulte Roth & Zabel**
(December 5, 2018, 3:39 PM EST)

One may find it difficult these days to read the news without encountering an article about cryptocurrencies, such as bitcoin and its brethren. While financial institutions, regulators and others are ambivalent toward cryptocurrencies' utility and ultimate value, most people are confident that blockchain, the technology that undergirds cryptocurrencies, may serve as a boon to a wide array of industries. Commercial real estate in particular may be one of its greatest beneficiaries.

What Is Blockchain?

Blockchain technology refers to a method by which information — both personal and commercial — is recorded and shared. Presently, the recording of such information occurs largely on paper or paper equivalent, such as a Word or PDF document. The information's provenance, authenticity and safekeeping are not always certain. Blockchain addresses these issues. In a blockchain network, all recorded information is traceable, agreed upon and permanent.

How Does It Work?

Think of the purchase of a secondhand car. Suppose Sally sends an email to Beth memorializing the terms of the sale of Sally's car to Beth: "On January 1, 2018, Sally sold Beth a Mazda, VIN# ABC123, for $15,000." The email is not conclusive proof that Beth purchased the car. First, we don't know whether Beth actually purchased the car — after all, only Sally sent the email. Second, even if Sally produced an email from Beth confirming the sale, we don't know whether Beth actually sent the email — Sally may have doctored the email. Third, it's possible, however unlikely, that Sally did not even send the email. Fourth, even if Sally and Beth sent the email, we don't know whether Sally had marketable title to the car. Fifth, even if Sally had marketable title and conveyed it to Sally, Beth's funds may not have cleared, or title may not have passed to Beth until a later date.

To solve these problems, imagine something called "magic email." In a magic email, the identity of the sender, recipient, copied parties and content are verified, consented to and permanent. Imagine further that the identity of the sender, recipient, copied parties and content of all forwarded magic emails are verified, consented to and permanent. Imagine that select portions, or the entirety of the email, can be disclosed to any party. And finally, imagine that the magic email and its content can be sent only upon the consent of the sender, recipient and all copied parties.

Let us return to the car sale between Sally and Beth. Suppose that Sally's email to Beth memorializing the sale was a magic email. Inasmuch as the email and its content could only be sent and received by the actual Sally and actual Beth, and only upon their approval, we are in a much better position to confirm the car sale.[1] In order to get to the heart of blockchain, assume now that this email was the last email on a magic email chain that was preceded by the following magic emails:

A magic email from Mazda Motor Corporation, the car's manufacturer, to David's Dealership, memorializing the sale of a car by Mazda to David, which contains the car's identification (VIN, make, model) and transactional information (parties, price, date of sale); and a subsequent magic email from David's Dealership to Sally, memorializing the sale of the car by David's Dealership to Sally, which contains all salient transactional information, and also contains the contents of the magic email between Mazda and David's Dealership.[2]

Sally is able to look up the magic email chain and note the provenance of the car. Now, with Sally's magic email to Beth at the end of the magic email chain, Beth may look up the chain and observe every detail of the car's transactional and title history. Beth's eventual purchaser will be able to do the same. Each magic email is a block of information comprising a chain (block+chain).

We can now transpose the magic email system to blockchain: Instead of email addresses, parties to a transaction establish a blockchain network. Each party's outlet to the network, through which it will interact with other networked parties, is called a node. Networks can either be private (permissioned), admitting invited participants only or public (permissionless) such as Bitcoin's blockchain network.[3] The content of a magic email to be shared on the blockchain network among the parties is recorded as a block of data on a ledger. The ledger is distributed to each node (party) on the network, and the ledger is synchronized in real time and at the same time to reflect any newly recorded information. Since everyone on the network has a copy of the ledger, everyone has the same and current information. There is no central database housing the ledger.

The block of data recorded on the ledger (the first block is called the genesis block) contains a set of informational blockchain system technical-related metadata, the specific transaction information, a time stamp and digital signatures of parties ratifying the transaction.[4] The information recorded on the block is converted into a hash, which appears at the end of the block. The hash is a series of numbers and letters, which confirms the validity and integrity of the initially inputted information.

Supposing a new transaction has occurred, a second block of information will be added to the ledger. Its top will have the same hash as the genesis block marking its order in the chain. The second block will contain all pertinent transactional information and conclude with its own unique hash based on the new input data. The hash, and the information it represents, is therefore the current state of events of the overall transaction. Crucially, the second block cannot be added to the ledger unless there is consensus by all network parties. Once there is consensus, the block will be created and added to the chain, and the ledger will be updated across every node. A third block of information, assuming consensus, will have at its top the second block's concluding hash (each block has two hash numbers except the genesis), which marks its place in the chain, and so on.

A hash is an indispensable component of blockchain technology. It is a string of numbers and letters, such as 00000000000000000034b8115d651ace734123d57a1965802677b6f53acb1515, which is generated by inputting the information to be recorded on the block into a hash function (similar to a junkyard metal compactor) which produces a hash. Regardless of the length of the input information, such as "Sammy sold 123 Maple St. to Barbara," or "Hello," a fixed length hash will be created. One of the safeguards of hashing is that only identical input data will produce an identical hash; if there is one change to the input data, the hash will, per force, be different. Therefore, the hash is the alarm that will be triggered if information is changed on a block. Suppose a transaction that has been recorded and hashed states "S sold to B a widget for $1,000" is changed to "S sold B a widget for $1,100." The changed language, input data, would create a new hash, which will not link to its preceding and succeeding counterparts. [5] The entire network would be able to observe the disruption and evidence of tampering.

If a recorded block contains a transaction information error, a new block must be added to the chain to reflect the desired change. The block in question is not changed as it would change the hash, thereby corrupting the entire series of hashes, and ruin the chain. This enables all parties to have a record of every action that was made in connection with a particular transaction.

Why the Sudden Interest in Blockchain?

To philosophize for a minute, rapid technological development has created a reality in which people must share their most sensitive personal and financial information with strangers. For instance, one must provide a Social Security number to a utility company representative on the telephone; one must display one's driver's license, which contains one's residential address and an identification number, to a gas station attendant in order to verify one's age and purchase cigarettes; one must read off a credit card number to a merchant on the phone. We cross our fingers and hope that the information will not be harvested. Such blind trust is often abused leading to devastating consequences. In our hyper-fast marketplace, trust is a necessary but weak link in the chain of commerce. Blockchain may replace this link by introducing a new method to interface with our reality in a secure and controlled method.

Application of the Power and Principles of Blockchain to Commercial Real Estate

Commercial real estate transactions are complex, with many steps. Some steps include due diligence, securing financing and municipal recording of documents. Costly inefficiencies exist. This article will focus on three areas that may be streamlined through blockchain technology: municipal document recordings, verification of borrower data, and loan and ancillary documents trigger events.

Municipal Document Recording

Municipal records offices are the repository of real estate ownership and security instruments. The content of these documents underlie the entire industry. The protocols to record, search and retrieve these documents vary across jurisdictions with broad ranges of user friendliness. By and large, the information is all there, but accessing it, understanding it and figuring its place in the chain of title can be challenging.

In some jurisdictions, documents are recorded and cataloged in the following manner: A document, such as a deed, is presented to the recorder's office. A member of the recorder's office scans it into an electronic database. Then, the same or another member manually inputs into another electronic database the key details of the transaction as listed on the document, such as the names of the parties, property address, type of transaction. This information is linked to the scanned documents. The purpose of this additional step is to allow the public to search for specific information related to the recorded documents.[6] Some jurisdictions repeat the process internally for their property tax bureau.

The scanned image and inputted information are stored essentially on top of related preceding information in reverse chronological order. This becomes, to some degree, the chain of title. Inefficiencies and the prospect for human error abound. Blockchain technology would enable the recording of information concerning a particular property to take place on one ledger in a sequential manner, without the need for double recording and the prospect of human cataloging error.

Recording the transactions on a blockchain network would take the following general form:

Suppose a buyer finances the purchase of a plot of land from the government for $100,000. The genesis block of information on the ledger would state that the government owns 123ABC Street, Town of X, State of Y and would conclude with a hash. The second block would contain the acquisition and buyer information, and would have at its top the same hash as the genesis block, thereby linking the two states of ownership and reflecting no gap in title. This block would conclude with a unique hash. A third block would be created, at the top of which would be the preceding block's hash, thereby reflecting no gap and claims to the property, and would contain XYZ Bank's lien information, concluding with a new hash, which would appear on the next block, and so on.

The bank is assured that there are no superior claims to the property because the bank can look directly up the chain to see whether any liens have been placed. The buyer is assured that there are no prior ownership claims to the property because she can look up the chain and observe all recorded title information. This recording method is more efficient and transparent than current practices.

Data Verification

A second area of CRE that may benefit from blockchain technology relates to data verification. Throughout the loan application, underwriting process and ongoing loan servicing, a borrower provides documents to the bank. These include personal net worth statements, bank liquidity statements, Social Security numbers, current property financials, financials of other properties, mortgage payment verification documents and others. The borrower typically self-certifies the information contained in the documents as true to the best of her knowledge, and emails the documents to the bank. This process relies on the trustworthiness of the borrower, those handling the information in the bank and the security of email. Both the lender and borrower are left vulnerable to the flaws of this system.

The lender is left vulnerable because the certified information may be false (either with or without the borrower's knowledge). The borrower is left vulnerable because the sensitive information in the email may be accessed by an unauthorized party, errantly sent to a wrong addressee, or misappropriated (by her own or the bank's employee). Other options, such as overnight or messenger couriers are expensive and do not solve for the problem of actual documents falling into the wrong hands.

Blockchain technology may close these security holes. On a blockchain network, a borrower's personal bank may share directly with the lender the borrower's personal financial information. Better yet, the borrower can direct the bank to share only the information necessary for underwriting. For instance, liquidity verification for the past six months and nothing else. The borrower does not need to show unrelated transactions that appear on a bank statement, such as private transactions.

Furthermore, the prospective lender can receive mortgage payment histories and other necessary information from different banks for other borrower-owned properties. There is no processing delay or cumbersome coordinating of efforts. Importantly, the information is sent in a targeted and secure method from the primary information-holding party to the requesting party. This eliminates fraud and inefficiencies and leaves parties better protected.

Triggered Events

Another area of CRE that may benefit from blockchain relates to tasks that one party must execute upon the occurrence of certain conditions set forth in the loan and ancillary documents. For instance, a lender may require a borrower to pay a late fee if the borrower does not service its debt on time, or a lender may require that a reserve account be replenished when the balance falls below an agreed upon amount. Additionally, a joint venture or syndication agreement may require payments to investors based on the satisfaction of return hurdles.

Blockchain may be helpful in this area. In addition to storing these agreements on a blockchain network, providing the attendant benefits discussed above, a smart contract may be deployed to automate the execution of these tasks. A smart contract is a set of instructions ("if, then" coding) that automates the consequential actions upon the occurrence of an event. At the outset of a transaction, parties enter a set of instructions into the smart contract. Once a coded event occurs, such as the missing of a debt service payment, the smart contract will automatically send the late fee payment from the borrower to a specified account.

In truth, some triggered events may be executed through efficient auto-debit functions. However, even a simple late fee debit may be performed more efficiently on the blockchain network and with greater consequence. For example, all parties on the network would see the triggered transaction and know a party is late in making its payment. Further, as mentioned above, another bank that is considering whether to refinance the loan or to finance an acquisition for the borrower may see for itself the entire transactional history related to a specific loan, and the borrower's overall observance of covenants. This expedites underwriting, clears back-office task logs and provides a better overview of the lender-borrower transaction.

Another example of the utility of smart contracts and blockchain pertains to a sponsor's return of capital and payment of profits to investors. The amount a sponsor must return often varies from one investor to another depending on the JV or syndication agreement. Additionally, there may be hurdles that must be met in order to trigger a specific payment. With the help of a smart contract, payments can occur instantaneously and simultaneously to the group of investors on the network. (Note, transaction details can be selectively revealed to participants on the network. Investors on a blockchain network would not know their counterpart's deal terms; it's not a one size fits all system.)

In our rapidly developing commercial marketplace, blockchain technology may enable the secure storage and transmission of information. We've finally caught up with ourselves, for now...

Jeffrey A. Lenobel is a partner and Aaron C. Retter is an associate at Schulte Roth & Zabel LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firms, their clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Depending on the jurisdiction, the passage of title to the car can also be effected on the blockchain network, similar to trading cryptocurrencies. In this context, liens may be recorded on the blockchain

network, which Beth could observe, and would tie into whether Sally has marketable title.

[2] The parties may decide which information to reveal to the other party. For instance, David need not reveal to Sally David's purchase price from Mazda.

[3] https://blockchain.info/

[4] Using asymmetric cryptography — with a public and private key — parties to a transaction can securely send and digitally sign documents. The idea is similar to a mailbox, which is publicly visible, but for which only one person has an access key. This topic and the advantages over a regular e-signature is outside the scope of this article.

[5] One would need to spend about half a billion years using the computing power of every computer that has existed and currently exists to cause two different sets of input data to produce the same hash (also known as a hash collision attack).

[6] The Cook County Recorder of Deeds (Chicago, Illinois) provides this information in greater detail (upon which this description is loosely based) and explains how it successfully piloted blockchain technology to drive efficient practices. The full report can be accessed here.