Expert Q&A on Blockchain Technology in Banking and Financial Services

PRACTICAL LAW FINANCE WITH TODD KORNFELD, JOSEPH GUGLIARDO, AND GREGORY J. NOWAK OF PEPPER HAMILTON, LLP

Search the Resource ID numbers in blue on Practical Law for more.

An expert Q&A with Todd Kornfeld, Joseph Gugliardo, and Gregory J. Nowak of Pepper Hamilton, LLP on blockchain technology and its implications for the banking and financial services industries.

WHAT IS A BLOCKCHAIN?

A blockchain is a type of database. At a basic level, it is as simple as that. What makes a blockchain different from most other databases is the way in which a user interacts with it. For example, common attributes of a blockchain database are that it is "distributed" and "self-proving."

Distributed means that copies of a blockchain can be kept and maintained by many people or organizations and no copy is the master or lead copy. Self-proving means that from merely looking at a blockchain, the user can tell whether the data in that blockchain is correct or whether it has been tampered with.

Blockchains can potentially serve at least two functions:

- First, a blockchain provides a self-contained record of a transaction or series of transactions.
- Second, a blockchain can serve as a store of value. A well-known example of a blockchain application is the cryptocurrency Bitcoin. Bitcoin uses blockchain both for recordkeeping and as a store of value because the entries in a Bitcoin blockchain have their own intrinsic value.

WHAT DOES IT MEAN TO BE A DISTRIBUTED AND DECENTRALIZED DATABASE?

The original creator of a blockchain creates the first entry in a blockchain. The original creator can then establish rules for adding new entries to that blockchain and can make it public and available for copying by anyone on the internet. After that anyone can create their own clone of that blockchain and, with the right software that implements the prescribed rules, that person can update that blockchain and make their updated blockchain available for anyone on the internet to copy. The process then repeats. This is essentially how Bitcoin got its start.

Not only is a blockchain a distributed database, it can be a database with preset rules for adding new data, and those rules may not be in the control of any one party. In other words, control of the blockchain is "decentralized." For example, updating the rules for Bitcoin requires a majority vote of the people with the right software and enough computer power to add a new Bitcoin entry. As a practical matter, no one person or organization is in charge of Bitcoin. It is a public blockchain. This structure makes sense because Bitcoin was intended to be a cryptocurrency without (much) government regulation.

Financial applications that use blockchains are most likely to use private or semi-public blockchains, in which only:

- Certain people or organizations can see the blockchain and/or update the blockchain with new data.
- One person or organization (or a limited group) has the power to update the rules that govern the blockchain.

HOW DOES A USER KNOW A BLOCKCHAIN IS CORRECT AND THAT ITS DATA HAS NOT BEEN TAMPERED WITH?

The key to blockchain technology is that it is self-proving. This means by merely looking at the data in a blockchain, a user can tell whether the data in that blockchain is correct or whether it has been tampered with.

As its name implies, a blockchain is built of blocks of data that are chained, or linked, together. Each time a new block of data is added, a complex mathematical algorithm is used to analyze that block of data and all of the prior blocks in that chain. The algorithms are similar to those used for data encryption. The result of that algorithmic process is a unique number. In essence, that algorithmic process converts the data in the blockchain into a code number. That number, usually referred to as a "hash," is appended to the end of the blockchain along with the new block of data.

If someone subsequently alters the data in the blockchain, anyone with the right software and enough computer power can "rehash" the data in the blockchain and discover that the data in the blockchain

does not match the hash appended on the end of the blockchain. That makes the blockchain a self-proving (in a decentralized system) distributed database.

WHAT HAPPENS IF DIFFERENT PEOPLE TRY TO UPDATE MULTIPLE COPIES OF THE SAME BLOCKCHAIN AT THE SAME TIME? HOW DO WE KNOW WHICH COPY IS CORRECT?

That is potentially a problem, and one that is similar to traditional problems with database concurrency and updating. However, there are ways to solve this problem. For example, Bitcoin uses a series of algorithms and rules to keep distributed copies of its blockchain in sync.

In the case of Bitcoin, however, the solution imposes serious limits on transaction processing speed. Bitcoin is slow because during the updating process, various algorithms are used to compare various public copies of the Bitcoin blockchain in order to determine which is the most recent and complete copy. Some of that time is wait time to see what other updates are being performed on other copies of the Bitcoin blockchain.

WHAT ARE SOME OF THE RAMIFICATIONS OF BITCOIN BEING A PUBLIC BLOCKCHAIN?

Anyone can see the Bitcoin blockchain and anyone with the right software can update it. One important point about Bitcoin is that it is intended to act as a store of value. Bitcoin entries are a form of money. They do not represent money in the traditional sense, such as the $25 deposited into a bank account that appears in the bank's records as a $25 deposit (a digital representation of fiat currency). In Bitcoin, the database entries themselves are actually money.

For Bitcoin to be useful as a store of value and to be useful for business transactions, potentially everyone needs access to the Bitcoin blockchain. Putting aside all of the widely expressed legal concerns about Bitcoin (for example, fears about its use for money laundering, drug dealing, tax evasion, and so forth), the fact that Bitcoin is a public blockchain makes it more difficult to design and implement. This also introduces certain limitations, such as the limitations on transaction processing speed.

However, there can be private or semi-private blockchains in which only certain people or organizations can see and/or update the blockchain data. These sorts of blockchains may have better transaction processing speed and perhaps better privacy and security than a public blockchain. Most current financial industry efforts seem focused on private and semi-private blockchains.

WHAT ARE SOME OF THE SECURITY ISSUES RAISED BY BITCOIN?

To use Bitcoin, the user needs to have its own set of keys that identify it for its Bitcoin transactions (similar to an ATM card and its related PIN). Bitcoin users keep their keys in electronic "wallets" that are provided by a number of services. Bitcoin users often use "Bitcoin exchanges" to exchange currencies such as dollars for Bitcoins. Unfortunately, Bitcoin wallets and exchanges have proven to be insecure in some cases, and people have had their Bitcoin keys or their Bitcoins themselves stolen.

The problem has not been with the Bitcoin's blockchain database. Rather, the problem is that Bitcoin wallets and exchanges are not always secure, allowing people to steal others' Bitcoin keys or Bitcoins. One solution is to have more secure Bitcoin wallets and exchanges. This problem is not specific to Bitcoin. Any platform that uses blockchain technology is going to have a similar need for a secure way for users to prove their identity.

This problem is not limited to Bitcoin, blockchains, distributed databases, or any other new, similar technology. As has been widely covered in the press, the Central Bank of Bangladesh lost US$81 million when someone broke into its accounts at the Federal Reserve Bank of New York via the SWIFT system. SWIFT is a system that is used by international banks to transmit messages related to funds transfers. In terms of security, SWIFT, which has been operating since 1977, was designed as a highly secure, private network. Even though SWIFT itself may be very secure and difficult to break into, anyone who steals a SWIFT member's keys can steal that member's money. Based on press reports, the Central Bank of Bangladesh did not follow best practices with respect to its SWIFT key security. There may have been other incidents in the past with SWIFT keys that received less publicity.

The takeaway, therefore, is that blockchains are not inherently insecure, but that users of blockchains must guard their access keys carefully, the same way people guard their ATM cards and PINs.

EVEN IF USERS CAREFULLY GUARD THEIR ACCESS KEYS, WHAT OTHER SECURITY CONCERNS ARE RAISED BY BLOCKCHAINS?

Blockchains are as safe or unsafe as any other computer application. One issue with Bitcoin and perhaps other fully public blockchains is that there is no master or "golden" copy of the blockchain. That means if someone does manage to break the core security of the blockchain, it may be difficult or impossible to determine which data has been tampered with.

However this is not an insurmountable problem. It is possible to design a public blockchain to have certain rules that require a trusted party or parties to keep a "golden" copy of the blockchain data. For financial applications, that trusted party could be a regulated clearinghouse, for example.

WHAT ARE SOME POSSIBLE USES FOR BLOCKCHAINS?

One possibility is using blockchains as a store of value, like Bitcoin or Ether. These are sometimes referred to as cryptocurrencies, because in theory they hide the identity of their owners and potentially avoid government regulation, including policy changes in the money supply that may cause inflation and deflation. However, cryptocurrencies have their own form of inflation, as new units are "mined." This is why the Bitcoin algorithm just "halved" the value of newly mined Bitcoins, as a preprogramed attempt to ward off inflation.

However, for a variety of reasons, it seems unlikely that Bitcoins and other cryptocurrencies will see widespread use in the near term. These reasons include the current limits on transaction processing speeds and concerns of both the government (for example, tax issues

and cryptocurrency's usage in illegal activities) and potential users (for example, security concerns).

More likely, blockchains will be used as recordkeeping tools, in particular recordkeeping for financial transactions. Beyond financial applications, we are seeing blockchain application testing across many different use cases, including real estate transactions, supply chain management, provenance tracking, personal identity tracking, energy grid optimization, and intellectual property tracking (for example, music royalties), among many other potential use cases.

WHAT ARE SOME EXAMPLES OF WAYS FINANCIAL INSTITUTIONS MIGHT USE BLOCKCHAINS?

One possibility is that a bank could keep its client's checking accounts on a blockchain. The bank could then give each client something similar to an ATM card to prove their identity for use every time the client paid a bill electronically or made a purchase.

While at first glance this may not seem like much of an improvement over the current system, a closer analysis reveals some clear advantages. One benefit is that when a payment is made, the other party can see the payer's blockchain and how much money it has in its account, eliminating overdrawn accounts and bounced checks. In addition, the balance in the payer's account would be accurate, eliminating any question regarding when a check is going to clear. Because the blockchain is separate from a user's bank, its checking account blockchain can be updated and transactions processed when its bank is unavailable.

However, it is unlikely that this application of blockchains will happen anytime soon. This is because the number of payments that pass through the checking account clearing system is enormous and there are many parties involved. That said, checking accounts on a blockchain may eventually be common.

WHAT ARE SOME OTHER POSSIBLE BLOCKCHAIN APPLICATIONS IN THE FINANCIAL INDUSTRY?

There are many potential blockchain applications in the financial industry. For example, companies could maintain their share registers through a blockchain. In fact, industry participants have already made considerable progress towards this goal. For example, last year Chain.com, a blockchain developer, used NASDAQ's "Linq" blockchain ledger technology to complete and record a private securities transaction.

In July 2015, Overstock.com conducted a private debt offering using blockchain technology. In addition, in December 2015, the SEC accelerated the effectiveness of a Form S-3 registration statement filed by Overstock.com under which the company disclosed that it might use blockchain technology in connection with a future offering under that registration statement.

Blockchain share registers offer significant advantages over the current system. Currently, almost all publicly traded securities are held in book-entry form, where a single share certificate in the name of a nominee represents the ownership interests of thousands and even hundreds of thousands of individual investors. Shareholder voting and investor communications are currently cumbersome processes, where materials must be forwarded by the nominee to its participant broker-dealers that must then forward them on, potentially using additional layers of broker-dealers, until they ultimately reach their beneficial owners. In this process, issuers have little information about who their beneficial shareholders are, except for the very largest shareholders who are required to make public filings with respect to ownership.

A blockchain could be an efficient and transparent method of addressing some or all of these issues. Blockchains might allow for same-day and possibly same-minute settlement of stock trades. In addition, blockchains might allow for more efficient recordkeeping, requiring less manual reconciliation, and perhaps smaller middle and back offices. Blockchains also have the added advantage that they may permit an issuer to more easily identify its shareholders and communicate with them.

A related issue is that the current share registration system does not interact well with existing federal securities law and state corporate laws, many of which were generally developed prior to the movement to book-entry share registration. For example, under the Securities Exchange Act of 1934, certain companies with fewer than 300 shareholders of record may essentially deregister, cease periodic reporting, and "go dark." Since many public companies have few shareholders of record, with almost all beneficial shareholders holding through book-entry, many public companies are potentially eligible to "go dark."

Since beneficial shareholders hold their shares through book-entry, certain companies incorporated in states such as Delaware that have been involved in proxy contests have refused to allow beneficial shareholders to nominate directors. They have apparently based such refusals on a combination of their by-laws or corporate charters and Section 219 of the Delaware Corporate Code, which defines the list of shareholders entitled to vote by reference to the company's share register and does not include the concept of book-entry beneficial owners. While federal securities law and state corporate laws are probably in need of amendment with respect to the concept of "shareholders of record," blockchain technology might be a good solution for all interested parties.

HAVE THERE BEEN ANY GOVERNMENT INITIATIVES FOR DEVELOPING BLOCKCHAINS?

Delaware has proposed making changes to its corporate code to encourage the development of a blockchain-based distributed ledger-based share ownership system. While still in its initial phases, Delaware Governor Jack Markell has announced his support for the creation of a new method of representation of corporate share ownership in which Delaware corporations will have the ability to issue and register shares using distributed ledger technology. Given the large number of Fortune 500 companies that are incorporated in Delaware, this initiative could quickly move the industry standard from book-entry to blockchain share registration.

HAVE THE BANKING AND FINANCIAL SERVICES INDUSTRIES BEEN DEVELOPING BLOCKCHAINS?

Most major banks and broker-dealers and many of their service providers have active blockchain projects. For example, based on published reports, a working group including Bank of America

Merrill Lynch, Citi, Credit Suisse, J.P. Morgan, and The Depository Trust & Clearing Corporation (DTCC) has been developing various blockchain-based settlement and recordkeeping systems for credit default swaps (CDS).

DTCC has also been working on blockchain systems for securities repurchase agreements (repos), which are commonly used by broker-dealers to finance themselves. The repo market is large, and many broker-dealers use it as the primary means for financing their operations. Yet, the repo market opens and settles trades in a disjointed and antiquated fashion, in which it is difficult to determine a particular bank's or broker-dealer's net exposure and credit risk at any given moment.

This lack of transparency has been a focus of federal regulators, which have been pushing for improved processing of repo trades. Regulators are concerned with potential losses by participants in the repo market. Blockchains appear to be a technological way to improve repo settlement risk transparency and reduce counterparty credit risk.

Industry participants have also discussed the possibility of prime brokerage or securities lending being performed using a blockchain. For example, each hedge fund could have its own blockchain and could then borrow securities from many industry participants – not just their prime broker. While this might raise a variety of issues, including privacy issues, some managers will likely choose to blockchain their hedge funds.

There has also been speculation that blockchains might serve as efficient, automated recordkeeping for, among other things, mortgages, land titles, marketplace (peer-to-peer) lending, and securities and commodities clearinghouses. Blockchains can potentially offer accurate recordkeeping, the ability to keep track of a chain of title, speedy settlement cycles, and the ability to embed smart contracts.

WHAT ARE "SMART CONTRACTS" AND HOW DO THEY RELATE TO BLOCKCHAINS?

A smart contract is a computer program that has the ability to take action, if contract terms are satisfied, without human intervention. Blockchains allow for the embedding of smart contracts.

To illustrate, consider CDS transactions. CDS are contracts in which one party pays a periodic premium to a second party and the second party makes a payment to the first party if an extrinsic event, such as bankruptcy, occurs with respect to a third party (Company Z).

In this example, the market could create a blockchain for CDS referencing the potential bankruptcy of Company Z. As investors traded CDS on Company Z, corresponding entries would be made in the blockchain. As periodic payments become due, smart contract technology embedded in the blockchain could automatically withdraw the payment from one party's bank account (which could be kept on a blockchain) and send the payment to the other party's bank account (which could also be kept on a blockchain).

In addition, if the embedded smart contract detects that Company Z has become bankrupt, then both parties to the CDS could be notified and the appropriate payment or payments could be made automatically. If there are insufficient funds to make a payment, then the embedded smart contract could notify both parties. If a periodic payment is not made within a specified time, then the embedded smart contract could deem the CDS contract in default and could calculate and demand appropriate damages.

Repos, securities lending, and many swap agreements seem well-suited for smart blockchains. Although often part of a larger, more complex package, prime brokerage for hedge funds and institutional investors are also likely to be suitable as smart blockchain applications. Potential applications could ensure systematic recordkeeping, reduce settlement cycles, and provide more advanced credit-exposure netting. As a result, participants could benefit from reduced capital requirements, faster trade execution with broader and deeper markets, and less systemic risk.

The inclusion of smart contract technology might also turn a blockchain into something resembling an exchange, such as a swap execution faculty (SEF) or a clearinghouse. For example, a smart blockchain could include not only recordkeeping and post-trade execution functions, but it could also include a request to enter into a trade. Market makers could then respond and fill the order request using the smart blockchain.

WHAT ARE SOME SMART CONTRACT APPLICATIONS?

Initially, it will probably be expensive to turn a paper contract into a smart blockchain contract. So the first applications might be those with many users and standard terms. Health insurance contracts might be an early adapter. The healthcare recordkeeping process is complex and burdensome, yet many people are covered under health insurance with the same terms.

In financial services, certain types of contracts, such as repos, which we've mentioned, and ISDA Master Agreements for swaps, generally have standardized terms and might be early adopters of smart blockchain contracts.

WHAT ARE SOME OF THE LEGAL ISSUES RAISED BY SMART CONTRACTS?

Smart contracts, whether in blockchains or otherwise, raise all sorts of interesting legal questions, such as:

- Which party is responsible for coding errors?
- Will contracts generally become more standardized, with boilerplate terms, in order to make smart contract implementation faster and cheaper?
- How are courts likely to treat and interpret smart contracts?
- What will happen if smart contract users are located in different countries?
- How will that relate to contracts that may be legal in one country, but not in another?

There are many legal questions with respect to smart contracts and blockchains, which will only be answered in the future.

RELATED CONTENT

Topics

- Swaps and Derivatives (1-500-0080)

Practice Note:

- Consumer Regulations Governing Emerging Payment Systems (7-608-7201)

Article

- CFTC Commissioner Giancarlo Discusses Implications of Blockchain for Financial Services (w-001-8928)

Legal Update: archive

- DTCC: Blockchain Could Revolutionize Financial Infrastructure (w-001-4062)
- Successful Blockchain Credit Default Swap Smart Contract Test Completed by DTCC Working Group (w-001-9268)