# Why bankers and lawyers need to understand blockchain and smart contracts

July 5, 2018

This article will discuss (i) how blockchain and distributed ledger technology ("**DLT**") and smart contracts will reshape the corporate lending space throughout the world; (ii) practical examples of near-term opportunities for the financial community to leverage this technology in a meaningful way; and (iii) the new roles that bankers and lawyers can play when using this technology.

## Blockchain and DLT is not to be confused with Bitcoin

When most people hear the terms “blockchain” and “DLT”, they immediately think of Bitcoin and other cryptocurrencies. This is not surprising due to the constant media coverage surrounding the meteoric rise in the value of the cryptocurrency market.

Many leaders within the finance community are sceptical and in some cases openly hostile to the long-term potential for cryptocurrencies to serve as a payment platform or a storer of value. Additionally, because the mainstream media often associates blockchain technology with cryptocurrencies, the financial community has not taken the time to explore the various use cases for blockchain. Blockchain and Bitcoin go together like computers and Facebook; just as you can do more with a computer than use it to check Facebook, you can do more with blockchain than just store Bitcoin.

Recently, the value of cryptocurrencies has stumbled and the ICO market has been targeted by regulators over questionable financings. As a result, the lending community has shifted their attention away from using blockchain and DLT as cryptocurrency platforms and is focusing instead on how these technologies can be used to record, govern and maintain complex financing transactions in an efficient, cost-effective and secure manner.

## Centralized database versus decentralized network

For most financial data, the world relies upon central intermediaries such as banks, accounting firms and governmental entities to create and maintain centralized, private databases, which keep track of such data and the transactions they comprise. In many instances, these databases are powered by antiquated, legacy computer systems that are inefficient, slow, costly and incompatible with other legacy systems. For most financial institutions, improving the customer experience has been their number one priority. Unfortunately, while the vast majority of banks and credit unions aim to compete and win new business by offering a personalized digital consumer experience that

removes friction, existing bank infrastructure  built on legacy systems may make this difficult.

A centralized database managed by one entity is susceptible to cyberattack and error and in some parts of the world, affected by political and state manipulation. Effectively, the central intermediaries, through their own private databases, determine (i) the status of each transaction; (ii) the ownership of certain goods; and (iii) the speed in which a transaction is completed.

Conversely, blockchain/DLT utilizes a decentralized, peer-to-peer network comprised of many users, which maintains a ledger of transactions and relies upon multiple users to confirm the veracity and authenticity of such transactions using cryptography. Blockchain essentially provides a “record book” of each component of a transaction and this record book is maintained and instantaneously authenticated on a network that is shared between a theoretically infinite number of computers. When all the members of the network approve a transaction, that transaction is added to the record book and such transaction cannot be tampered with or altered.

# Benefits of a decentralized network within a financial institution

## Elimination of mistakes/single source of truth

With the current, centralized model there is only one entity that is the “record-keeper” of data. If there is any issue with the system or the people running the database, the data is exposed to error, as there may be no verification system to monitor the data. Conversely, a decentralized database is comprised of multiple record-keepers who keep track of the same data. These record-keepers are known as “nodes.”  A decentralized network is essentially a network of nodes, which all maintain a single ledger, and this ledger keeps track of the same set of data.

Every node on a decentralized database operates on the same software. Accordingly, anytime data within a decentralized ledger is transferred, the software running on each node that is connected to such decentralized ledger will automatically reflect the transfer of such data on the ledger of each node.

Instead of a single financial institution maintaining the data on a ledger in an isolated manner, the network of computers/nodes in a decentralized network can jointly monitor whether the ledger was updated correctly and flag any mistakes. The use of multiple nodes maintaining data integrity of a decentralized ledger decreases transcription errors and a real-time verification system ensures that the ledger is correct and accurate. Furthermore, the increased accuracy of the financial data would lead to a significant reduction in disputes and needless litigation.

When you consider a typical syndicated lending transaction, (operating under the current centralised model) comprised of multiple financial institutions, each institution would store the specifics of such syndicated transaction within its own ledger. This ledger would be updated manually and each institution’s ledger would function on its own proprietary operating system. Conversely, if the same syndicated financing was recorded on DLT, the entire lending syndicate would use the same ledger to monitor the transaction such that once an amendment is made, it would be automatically replicated in real-time across the entire decentralized database.

## Public or permissioned-based DLT – Increased data security

It is important to note that DLT can be set up as a public decentralized ledger or a permission-based decentralized ledger. The decentralized ledger underlying Bitcoin is accessible by the entire world and accordingly it would be an example of a public DLT system. Conversely, a permissioned-based network is only accessible to specified entities who have received access to the DLT system.

Although a public decentralized DLT system is comprised of millions of nodes, which eliminates the potential for a

single point of failure (which is an inherent risk in a centralized model), financial institutions are wary of allowing the public access to a network that maintains confidential client information, even in encrypted form. Because of the sensitivities surrounding client information, financial institutions have focused most of their time and energy on exploring the potential uses of permission-based DLT systems. In these systems, the consensus process is regulated by a pre-determined set of financial institutions (the consortium) and each financial institution may act as a node on the decentralized ledger. Each transaction occurring on the ledger would have to be verified and validated by each bank comprising the consortium.

One of the most prevalent threats to financial institutions is data breaches. Despite the massive amount of resources invested by the financial community into securing their confidential data, the frequency of data breaches continues to rise throughout the world. This is to be expected as the perpetrators of data theft recognize the immense monetary value of accessing the records of financial institutions. Accordingly, they will go to increasingly sophisticated lengths to access such data. When confidential client data is managed by a single entity, a hacker only has to focus on hacking the ledger of that one entity.

Conversely, when a DLT platform is used to maintain client data, such data is distributed across peer-to-peer networks that are continuously updated and kept in sync. Because the data in a DLT system is not contained in a central location, it does not have this single point of failure. Instead, an ambitious hacker would require massive amounts of computing power to hack every node within the peer-to-peer network and alter the records of each node all at the same time. Because of this robust data security, DLT is often described as immutable and not susceptible to attack by hackers.

# Interchange between DLT and smart contracts

## What is a smart contract?

The term “smart contracts” was originally coined by cryptographer Nick Szabo in the early 1990s. Szabo saw a contract as a set of promises agreed to by a meeting of the minds. First, the contract terms are negotiated by the parties. Second, the contract terms are translated into computer code using “if-then” functions (conditions). Finally, the code is embedded into a decentralized DLT system and monitored and maintained by a series of nodes. Once a condition is met, the smart contract will take the next step necessary to execute the contract. Thus, the term “smart contracts” refers to computer transaction protocols that execute the terms of a contract automatically based on a set of conditions.

> A simple example of a smart contract would be the following:
>
> Bank A lends $1,000 to Bob. Bob promises to repay Bank $1,050 on September 1, 2018. Computer code is generated to represent the following if-then function:
>
> If on September 1, 2018, Bank A does not receive $1,050 from Bob, transfer $1,050 from Bob’s account to Bank A’s account.

The above computer code would be deployed on a private network, which would include the computers of Bank A, Bob and Bob’s depository bank. Bank A and Bob would sign a coded contract, otherwise known as a smart contract.

Many of the DLT platforms being developed within the financial industry (CORDA, Ethereum Virtual Machine, Hyperleger Fabric, etc.) have been developed to allow smart contracts to be embedded within their infrastructure.

Because smart contracts are self-executing without human oversight and reconciliation, their use in the financial services industry could dramatically reduce costs for financial institutions. An often-cited potential use case for smart

contracts is found within the Anti-Money Laundering (**AML**) space, as financial institutions are required to verify and identify their clients in order to comply with AML laws and regulations. This process, called "Know Your Customer" (**KYC**), is costly and inefficient. Smart contracts could be designed and used by a syndicate of lenders to automatically, rather than manually, check and verify customer information against approved central records. Additionally, because the distributed ledger has a history of all conducted transactions, it will be able to detect questionable spending patterns of a potential client that may be engaging in illegitimate activity.

A more complex example is a smart contract coded to release money to a borrower the moment a mortgage is registered. Once the smart contract detects (i) the borrower is the registered owner of the mortgaged property, and (ii) the mortgage has been registered in first position on the applicable land registry, the financing proceeds would automatically transfer to the borrower's bank account. Besides ensuring the mortgage is registered, the computers could regularly check whether the borrower maintains (i) a certain credit score level, and (ii) employment with a specific employer.

## Will smart contracts replace lawyers?

Yes and No. Smart contracts will change the role that lawyers will play in certain commercial transactions and, in many cases, reduce their role. For example, through the use of smart contracts, lawyers may have a lesser role in registering and transferring assets, verifying the completion of certain conditions precedent, monitoring covenant compliance, registering and discharging security and many other areas that can be replaced by self-executing computer code. However, the major limitation facing the implementation of smart contracts and distributed ledger technology into the loan agreement is that these very complex and heavily negotiated agreements must be coded. One of the main challenges facing smart contracts is the difficulty of combining the technical computer code written by computer coders with written legal prose drafted by lawyers and doing so in a standardized and seamless manner.

There are different ways to configure a smart contract, which will depend on the complexity of the transaction being represented. On the one hand, for binary, well-defined agreements, it is possible to replace the entire legal contract and convert it to computer code for self-execution. However, for more complicated commercial transactions, it will be necessary to bifurcate the contract such that some of the terms of the contract are represented by computer code written in the form of a smart contract and the other, more nuanced elements of the contract are represented by traditional legal wording. In a syndicated financing for example, there are elements of the credit agreement that are binary, such as the following: if the Borrower receives a certain credit rating from one of the major credit rating agencies, the Borrower's loan pricing will move to a certain level. This is the type of if-then scenario that could be coded and included within the portion of the credit agreement documented within the smart contract. Conversely, a typical syndicated credit agreement will contain provisions which include qualifiers such as "materiality," "reasonableness," "best efforts basis" and "material adverse effect," each of which are concepts that are nuanced and cannot be easily converted into computer code. It appears that smart contracts will represent an incremental evolution of the legal industry and not a replacement.

## Next steps for bankers and lawyers

It is inevitable that DLT and smart contracts, in some form and variation, will become part of the financial services industry. There is simply too much competitive pressure on all parties to reduce costs, increase efficiencies and expedite processes to ignore this technology. Accordingly, the question is not *will* this technology be adopted, but instead (i) at what pace will this technology be adopted, (ii) what permutation of the foregoing technology will be implemented industry wide, and (iii) what skill-sets will bankers and lawyers need to stay relevant in this evolving market?

Going forward, bankers and lawyers will need to pay close attention to the technology that is adopted by the financial services industry, which will no doubt be a combination of some form of DLT/smart contract system. Further, bankers

and lawyers will need to keep an eye on how their role will evolve as this technology is adopted and ensure that they are “coding literate” and knowledgeable about the principles of DLT and smart contracts.  Because of the diverging skill-sets between a typical lawyer and computer programmer, there will no doubt be great opportunities for intermediaries and/or software programs to enable these divergent service providers to work together.

---

This article was co-authored by Ilan Levy, a summer student in the Toronto office.

# Your Key Contacts

**Ryan Middleton**
Partner, Toronto
D +1 416 361 2367
ryan.middleton@dentons.com