THE REVOLUTIONARY POWER OF BLOCKCHAIN — AND WHAT IT MEANS FOR BUSINESSES AND LAW FIRMS

In the last two decades, the emergence of transformational, industry-disrupting technologies has almost become routine. Big Data, automation, cloud computing and other technologies have changed the very nature of business.

These shifts, profound as they are, herald merely the beginning of a new era of digitally-powered advances. More new technologies are poised to create even greater changes. While driverless cars and virtual reality garner most of the headlines, few advances have more potential to upend the way business is conducted than blockchain—the technology that underpins Bitcoin and other cryptocurrencies.

Don Tapscott, one of the world’s most prominent business and technology thinkers, has observed that blockchain has the capacity to revolutionize the world economy by ushering in an era of unmediated, peer-to-peer transactions. This transaction model will open new markets and dramatically lower the capital requirements necessary to start a business.

Blockchain can also fundamentally change the way state governments handle procurement and other financial transactions or services. Governments can use blockchain to manage public or private records or monitor the transfer of property. These services will lead to greater accuracy and transparency, creating greater trust between citizens and their governments.

The legal industry, too, is well-positioned to benefit from blockchain. Contract drafting, enforcement, administration and other core legal functions could all be transformed by the adoption of blockchain technology.

Before delving any deeper into these impending changes, it’s necessary to take a closer look at the fundamentals of blockchain technology, how blockchain departs from the traditional transaction model, and how blockchain models themselves differ from one another.

continued on page 2
THE ESSENTIALS OF BLOCKCHAIN

The easiest way to grasp the essence of blockchain is to imagine a ledger—one that’s digital (such as an Excel spreadsheet), rather than paper-based. Much like on a standard ledger, transactions are written and stored on a blockchain. Information about financial transactions (or other important data) is then distributed across millions of computers, potentially. In this sense, a blockchain is like a massive global spreadsheet that anyone can see and alter.

What makes blockchain truly remarkable, is that its design—while open source—is also exceedingly difficult to corrupt. In addition to the strong encryption of all data, blockchain databases are not stored centrally, but are instead stored across vast numbers of computers and are publicly accessible. In order for someone with malicious intent to hack the blockchain, every site with access to the ledger would need to be hacked simultaneously, and the exact same data would need to be altered.

While security is certainly one of blockchain’s key benefits, it’s not the only radical change the technology promises. To understand how blockchain’s shared distribution model differs from traditional models, imagine a Word document being shared and edited by several people. While one person makes edits, the other users are precluded from doing so; they are locked out and cannot see or effect changes. This model has drawbacks; primarily, it’s easy to lose track of alterations, which can lead to errors.

A distributed ledger, on the other hand, offers full access, all the time. It’s an asset database (financial, legal, electronic or physical) that can be shared and synchronized across networks spanning multiple sites, locations and institutions. Everyone in these networks has access to their own copy of the ledger and changes are reflected in minutes, if not seconds.

“As the technology matures and grows more refined, greater capabilities, lower costs and increasing rates of adoption could generate enough momentum to make blockchain the next “traditional” transaction model.”

The most prominent example of this model is, of course, Bitcoin. Yet the underlying technology has far-reaching applications that extend well beyond digital currencies. Blockchain can be used to create wills, sell personal items or even discover the provenance of jewels. Blockchains do not merely reflect a record of who paid whom; they can contain any structured data (who owns a particular plot of land, for example). This potential for vast, wide-ranging applications is what makes blockchain so exciting.

Distributed Ledger

Distributed network with all nodes on the network able to transact
No need for designated intermediaries
Multiple copies of same information across all systems in the network

continued on page 3
WHAT CONSTITUTES A BLOCKCHAIN?

While blockchain is a type of distributed ledger, it’s important to realize that not all distributed ledgers are blockchains. The fundamental distinction lies in the way data is recorded.

In its simplest form, a block within a blockchain is some form of information: contracts, proofs of financial transactions, ownership records, computer code and so on. Each block in the database is securely chained to the preceding and proceeding block via a digital signature (or a “hash”); this process is called a “hash function”.

Blockchains grow longer and more complex as more information is added to the database. However, because all changes are visible, everyone in the chain can immediately see unauthorized changes and judge their validity.

Simple Blockchain Structure

**Proof of work:** This is an ID referred to as a hash composed of a random set of encrypted numbers and characters. Each block within a chain link is linked with its previous and proceeding block.

**Transactions:** Each block can contain one or multiple transactions.

**Public Key:** The public key identifies the sender and receiver within a transfer of information.

TRADITIONAL TRANSACTIONS VS. BLOCKCHAIN TRANSACTIONS

Much of blockchain’s revolutionary potential lies in how it departs from the traditional transactional model. Historically, transactions have required a third-party to be completed or put into action. In the case of a customer paying her cable bill by check, for example, the bank serves as the third party, or approver. Third parties, such as banks or government agencies, also act as authenticators and record keepers, and in this way enhance trust and credibility. This is particularly critical in terms of digital transactions, as computer files are easily reproducible, and there is the potential for assets to be sold more than once.

Yet, there are distinct drawbacks to the traditional model. The presence of fee-charging middlemen—perhaps even multiple layers of them—makes transactions more expensive. Additionally, third parties are open to liability concerns should errors occur during a transaction as a result of mismatched information.

Blockchain avoids these problem areas by upending the traditional model and dispensing with the need for a special third party to approve, authenticate and record transactions. Because the blockchain is visible, anyone in the network can act as an authenticator or approver.

One example of this is a standard Bitcoin transaction. Here, one person pays another directly, with no intermediary. Bitcoin acts as digital cash that is sent directly to a vendor for a product or service, while no identifying personal data (such as a credit card number) is required. Additionally, because no third party is involved, the seller does not have to pay the standard processing fee associated with the traditional model.

continued on page 4
The potential of blockchain extends beyond simple online transactions. In a world where blockchain technology is widely adopted, property rights would be easily established; dividends and other corporate functions would be automated and entirely accurate; securities lending records would be highly accurate; capitalization table management would become far easier and proxy voting would be transparent and error free.

Additionally, blockchain technology would provide these core benefits:

- Automation would lead to lower costs
- Having no centralized point of attack would greatly improve network security
- The system would ensure compliance to the legal code, withholding any discrepant transactions
- Information would remain consistent across all systems, eliminating the need for parties to maintain and reconcile individual copies
- All transactions would be permanent, as the system would not allow duplication, deletion or alteration of approved transactions

While the promise of those benefits is truly profound, there are some very real challenges that must be addressed before blockchain technology is implemented on a wide scale. These challenges include:

- Like many new, disruptive technologies, the initial outlay in terms of cost and resource deployment is high
- While security is strong, it is not impenetrable
- Low system power makes it impossible to process more than a few hundred transactions per second
- The technology is young, and as such vulnerabilities and limitations are not fully understood

Though blockchain technology has truly transformational potential, it’s important to be cognizant of these challenges. As the technology matures and grows more refined, greater capabilities, lower costs and increasing rates of adoption could generate enough momentum to make blockchain the next “traditional” transaction model.
BEYOND BITCOIN: USING BLOCKCHAIN FOR SMART CONTRACTS

While blockchain was created to service Bitcoin transactions, the applications of the technology have long outgrown that narrow mandate. Because it can be used to track and record anything of value, blockchain has enormous market utility—and smart contracts are one example.

For the uninitiated, smart contracts feature terms written in programming language, rather than legal language. These contracts are automatically executed by a distributed ledger or computing system of comparable design.

There are a variety of potential uses for smart contracts. One example: During a real estate transaction, smart contracts can transfer a title or release escrow once ownership is verified. This, in turn, greatly lowers costs related to insurance and transactions. Additionally, contracting, enforcement and compliance costs are reduced, making it economically feasible to create contracts over numerous lower value transactions.

In this way, smart contracts and distributed ledgers have a potent synergistic effect; when the two are paired, the combination is powerful enough to automate many financial services.

Risks, however, do remain—and foremost among these is total reliance on a computing system to handle contracts. Because the technology supporting smart contracts is still embryonic, most risks and benefits remain theoretical. There has been movement to grant smart contracts the same legal effect, validity and enforceability as traditional contracts, with Arizona recently becoming one of the first U.S. states to grant that status.

Smart Contracts Advantages

- Contract stored on the network, with transacting parties able to access the network through their respective systems and encryption keys.
- Since the contract on the network is coded in system language, it can be executed by the network.
- Users can withhold or freely share their information with other members (with access keys) in the system.
- Contract execution can be automated. Also any changes are updated in real-time across all systems.

continued on page 6
THE REVOLUTIONARY POWER OF BLOCKCHAIN — AND WHAT IT MEANS FOR BUSINESSES AND LAW FIRMS

BLOCKCHAIN DATABASE APPLICATIONS: PUBLIC, PRIVATE AND CONSORTIUM

To help better illustrate the functionality of blockchain database applications, let’s take a closer look at the three main types: public, private and consortium. These three categories refer to the degree of which a blockchain system is open or controlled.

Public blockchains
Perhaps the best example of a public blockchain is Bitcoin. There are no restrictions on who can participate; anyone can mine for Bitcoin and anyone can conduct transactions. The primary benefit of this public setup is that no company or individual can control access to information on the blockchain or the rules governing the blockchain. The owner of the blockchain may not take unilateral action to change the blockchain to the detriment of the users; meanwhile, information is authenticated by virtue of an agreement among users.

While the public nature of this database may seem less secure, there is no agreement among experts as to whether that is the case. Privacy issues, however, are another matter. It remains an open question as to how much transparency regulators (or users) will accept with regard to blockchain transaction or event records, and how privacy concerns will be addressed.

Private blockchains
If a public blockchain resembles the accessible, free-wheeling Internet in some respects, a private blockchain has more in common with the closed ecosystem of a corporate intranet. These blockchains are only accessible to those given permission by the operator. In this sense, private blockchains are essentially private databases structured as distributed ledgers.

For some organizations, this closed, private structure is a core advantage, as it maintains confidentiality with regard to transactions on the chain. It also prevents sensitive information from being accessed by anyone with an Internet connection.

Some pro-public blockchain observers, are critical of this approach. By keeping transactions cloaked in confidentiality, private blockchains could be manipulated without raising awareness, as confidential transactions would provide cover for malicious actors.

Consortium blockchains
A middle-ground, hybrid alternative to public and private chains is the consortium blockchain. Here, the consensus process is controlled by a pre-selected number of nodes. For example, 15 financial institutions may jointly operate a chain, and each control a node. Ten of these institutions then must sign a block for the block to be valid.

The right to read transaction data may be either public or private. There are also options where the blockchain is designed in a way to allow public users a limited number of queries and get back cryptographic proof of a limited part of the blockchain.

Because of its setup, the consortium blockchain is considered partially decentralized.

CONCLUSION
In some respects, blockchain technology is elegantly simple. It also has the potential to represent a true paradigm shift—one that fundamentally transforms the finance industry, while having profound implications for other fields, such as law. Unmediated peer-to-peer transactions could radically lower the cost of doing business, reduce the barriers to entering business and allow governments, corporations and other entities to deliver services with greater accuracy, speed and security.

By understanding the essentials of blockchain, and how the technology is likely to develop in the future, law firms and corporations are well-positioned to reap the benefits generated by this new approach—and to carve out a significant competitive advantage.

LEARN MORE
To learn more about how CT can help you better manage your compliance requirements, contact your CT representative or call 855.316.8948 (toll-free U.S.).