Client Advisory

CARTER LEDYARD & MILBURN LLP
Partners for Your Business®

Cybersecurity Practice Group

July 11, 2017

Blockchain (Distributed Ledger) Technology: An Introduction

Blockchain (distributed ledger) technology is the software that powers Bitcoin. The technology is elegant, and a stampede of well-funded, smart technology companies and organizations (e.g., Microsoft, IBM, Intel, the Linux Foundation), financial institutions (e.g., Fidelity, BNY Mellon, BlackRock, JP Morgan Chase), numerous startups and consortia are developing adaptations for uses besides crypto-currencies. Over $1.7 billion has been invested in this effort so far. Every week enthusiasts in the financial services and commercial industries report successful proofs of concept and pilot programs to test applications of this technology, and many predict that eventually it could be as disruptive as the internet. Skeptics complain about the hype and point to the many barriers to wide-spread adoption.

Whether or not this technology turns out to be the Next Big Thing, a lay person should have some familiarity with what it is, what it might be used for, and what is slowing down its adoption.

What is blockchain (distributed ledger) technology? A technical person might define a blockchain as "a distributed database that maintains a continuously growing list of data records hardened against tampering and revision, even by operators of the database. The database is time-stamped, and contains the entire logged history of the system. Each transaction processor on the system maintains its own exact copy of the database, and the consensus formation algorithms enable every copy to stay in sync."

A less technical description of a blockchain is that each participant in the network has exactly the same copy of each immutable data file in a series of immutable data files, and a new data file can only be added to the series if a sufficient number of participants in the network agree that the new data file is valid. Many on-line resources provide helpful and accessible explanations by metaphor, such as "Blockchain Demystified" by Westpac Banking, and others show how a blockchain works, such as "Blockchain 101" by Anders Brownworth.

What makes this technology so appealing? Distributed ledger technology permits decentralization of information in a reliable form that updates virtually instantaneously, cheaply and confidentially to each participant in the network, and can be used in situations where network participants don't know or trust each other. A big attraction of the technology is the possibility of disintermediation, replacing official central record-keepers and thereby reducing the cost and increasing the speed of disseminating new information to all participants in the network simultaneously. Another attraction is the possibility that some interactions among group members can be automated using self-executing "smart contracts," as described below.

What applications of this technology are in the works? Distributed ledger technology is already in wide use to power crypto-currencies such as Bitcoin and Ether. The financial community is developing many other applications, like applications to make payments and enable foreign exchange trading; to implement trading of securities; to handle payment, clearing and settlement of securities trades; to handle lending of securities as collateral; to handle the initiation and mechanics of syndicated loans. One commercial application is the documentation for the cross-border purchase of goods and payment for them. Ownership of assets could be documented using distributed ledger technology; for example, legislation is pending in the State of Delaware that would permit use of the technology for recording ownership of shares of Delaware corporations; if enacted, this change would affect various legal rights of shareholders including voting and appraisal rights. Looking further into the future, individuals' medical records might be maintained using distributed ledger technology, so that persons with appropriate permissions would have the ability to view a patient's complete medical history without the need to conduct new medical tests or to create and maintain expensive duplicate medical records; additional medical tests and procedures could be added to the patient's medical records and made available virtually instantaneously to all persons with appropriate permissions.

Another application of the technology is the so-called "smart contract." A smart contract is self-executing: when stated conditions have been confirmed as satisfied, then stated consequences would automatically be implemented without any need for further human intervention. An example is a smart contract for the purchase, transport and delivery of goods across national borders. The contract could provide that after the lending party has entered a block in the contract chain reporting that financing for the purchase of goods is available, and the seller's shipping agent has entered a block in the contract chain indicating that the shipping agent holds bills of lading for the goods shipped, and customs officials or a customs agent have entered a block in the chain that the goods have cleared customs, the contract would automatically cause payment to the seller.

What's the current status of adopting this technology? All of the financial applications and the commercial purchase-and-sale application described above have completed successful proofs-of-concept and are now in pilot testing. Recording ownership of corporate shares is further off, and using the technology for medical records is further off still.

Despite the technical progress, many disagree on when the technology will be adopted, or whether it ever will be.

What are impediments to adoption of this technology? There are several impediments to wide-spread adoption:

- Regulatory authorization. Many applications involve regulated transactions such as the purchase and sale of securities, and post-sale payment, clearance and settlement. Financial regulators such as the Federal Reserve Bank, FINRA, the Bank of England and the U.K. Financial Conduct Authority have all published interim reports or discussion papers considering the risks and benefits of adopting the technology. These

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

agencies are likely to move slowly and will not authorize applications using the technology until they are satisfied that it will protect consumers and investors, protect privacy, preserve cyber-security and protect the integrity of financial markets.

- Governance. Participants in a network must decide how the network will be administered, how any problems and anomalies will be addressed, and how operating rules will be adopted or changed. Participants in many networks will be competitors, and they will naturally be reluctant to cede authority or share information with each other.
- Standardization. In the early stages of any disruptive technology, different versions compete for general adoption. Over time, one or a few of the possible versions will be adopted and the other versions will wither away. There are several well-funded consortia working feverishly on competing versions of this technology right now and only a few will survive.
- Acceptance by all relevant stakeholders. Some applications are only relevant for a few parties (the parties to a syndicated loan, for example), while other applications involve thousands or tens of thousands of parties (securities exchanges and broker-dealers, for example). Implementation of a new technology is expensive and requires personnel adept at using it. Participants will resist the additional cost unless they become convinced that the benefits in speed and cost-saving will justify the cost of adoption in a commercially acceptable period of time.
- Assurance of confidentiality, privacy and security. The raisons d'etre for this technology are its claimed confidentiality, privacy and security. If mechanisms were developed to hack a blockchain and counter-measures were not developed quickly, the impetus to adopt the technology would be compromised.

When will this technology be adopted? In fact, this technology has been in use since 2009 when Bitcoin was first distributed. Its staying power in a rough-and-tumble international environment suggests that the technology is sturdy and here to stay.

Prospects for cost saving and improved efficiency seem compelling. Further, at this point the idea has taken on a life of its own -- so many leading institutions have devoted so many resources to commercializing it that it's hard to see them walking back their commitments. On the other hand, the technology is doubtless being overhyped, and it's unlikely that all the benefits claimed for it will be enjoyed any time soon.

Applications will be adopted as quickly as the barriers to adoption can be overcome. Applications with few participants (a loan syndication, for example) will be able to do this fairly quickly, while applications that involve more stakeholders (securities trading and post-trade activities, for example) will take longer because it will be necessary to get competitors and regulators on board. Be that as it may, it is likely that some new applications will be adopted later in 2017 and this trend will continue well into the future.

There are fascinating conceptual and legal questions about this technology which will be covered in subsequent Client Advisories.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232

CARTER LEDYARD & MILBURN LLP
Partners for Your Business®

For more information concerning the matters discussed in this publication, please contact the authors **H. Thomas Davis, Jr.** (212-238-8850, davis@clm.com) or **Matthew B. James** (212-238-8644; mjames@clm.com), or your regular Carter Ledyard attorney.

2 Wall Street, New York, NY 10005 212-732-3200 Fax: 212-732-3232