EVERYTHING YOU NEED TO KNOW ABOUT
DIGITAL LEDGER TECHNOLOGY, THE BLOCKCHAIN AND CRYPTOCURRENCIES©
(Part I – June 2018)

Robert C. Brighton, Jr.
Brighton Legal Solutions P.A.
rcbrightonbizlaw@gmail.com

This is the first in a continuing series of blogs on digital ledger technology, the blockchain and cryptocurrencies.

Unless you have been hiding under a digital rock you have heard the terms "distributed ledger technology," "the blockchain" and "cryptocurrency"(or at least the term for the most famous cryptocurrency – bitcoin). Although most people have heard these terms, few people know what they are or know how they work.

In a series of blogs, I will explain some of the key elements of digital ledger technology, the blockchain and cryptocurrencies, including the evolving regulatory regime that is emerging.

Why should you care enough to spend your precious time to learn about distributed ledger technology, the blockchain and cryptocurrencies? Well, in short, it's because these digital developments will bring the greatest change to our business and personal lives since the Internet. They represent a more flexible, dynamic and efficient digital future. And that future is arriving faster than anyone would have predicted only a few years ago.

First the basics:

What is Distributed Ledger Technology?

In distributed ledger technology (DLT) information is replicated and shared among computers ("nodes") that are linked together in a network. By replicating and sharing an identical copy of the information, the nodes validate the information for a transaction by a consensus of a majority of the nodes,[1] and in this way collectively determine the validity (or lack of validity) of a transaction before storing the information in a permanent record. The key distinction from traditional ledgers used in transactions is that the information is not maintained and controlled by a central authority. Changes to the ledger are constructed independently and only become part of the permanent ledger after reaching consensus.

What is the Blockchain?

The blockchain is one form of distributed ledger technology. While every blockchain is a distributed ledger, not every distributed ledger is a blockchain.

[1] The consensus occurs automatically by use of a consensus algorithm.

The blockchain is a distributed ledger database grouped together in append only transaction records that are linked together cryptographically in blocks.

The blockchain provides answers to two problems that have plagued business, government and society generally since the dawn of history: security and efficiency.

Blockchain addresses security in two ways: (1) once created and linked, the record of information cannot be altered or withdrawn and (2) the append-only and shared nature structure of the ledger requires that each change in a link (the digital record maintained on each computer) can only be accomplished by a consensus of the nodes. Accordingly, the greater the size of the chain, the more formidable the task faced by someone seeking to make an unauthorized change since any attempted change is transmitted to every participant in the blockchain. This is not to confuse the security and safety of the public blockchain with hacking of private blockchains having a central administrator (more about the distinction between private and public blockchains later). This can and has occurred.[2]

---

[2] Generally, hackers have not directly broken into the basic code of the blockchain. However, in August 2010 in the first reported hack, a hacker managed to manufacture 92 million in bitcoin by identifying and exploiting a flaw in bitcoin's code (bitcoin is built on top of the blockchain; more about this distinction in my discussion of cryptocurrencies below). Fortunately, the bitcoin community were able to cancel all of the transactions and rollback the blockchain to its pre-hacked state.

In 2016, hackers attacked Bitfinex, a cryptocurrency exchange, and stole 120,000 bitcoins by using an opening provided by some poor coding in Bitfinex's multi-signature wallets (more about wallets below and in future blogs).

The largest loss suffered in a hack to date occurred in February 2014 when hackers stole 850,000 bitcoins over a three year-period from Mt Gox, at the time the largest cryptocurrency exchange handling about 70% of all bitcoin transactions. Mt Gox's clients suffered 750,000 of these losses. Hackers were able to edit transaction details hiding the theft. This was the second time Mt Gox was hacked, with the first occurring in 2011 when a computer belonging to one of its auditors was compromised enabling the hacker to alter the nominal value of bitcoin to one cent.

Probably the most famous (infamous) hack was of the DAO (an unincorporated "decentralized autonomous organization") in June 2016 as described in the case which resulted in the Securities and Exchange Commission (SEC) issuing a report (the DAO Report) detailing its investigation into the violation of federal securities laws by the DAO and others. I will discuss the DAO Report, as well as the hack, in a later blog. The DAO hack involved Ethereum and resulted in the soft fork (see discussion of forks below and in a later blog) of Ethereum, with the old Ethereum now called Ethereum classic and the forked version being called Ethereum.

The most recent hack of significance occurred in January 2018 when Coincheck, a cryptocurrency exchange, was hacked and 500 million in NEM coins (about 5% of the total supply of this cryptocurrency) were stolen. The hacker seems to have broken into Coincheck's network, but the details are still under investigation.

The most significant aspect of a hack of a cryptocurrency exchange is its effect on the psychology of the market. After a recent hack of the South Korean cryptocurrency exchange Coinrail in early June 2018 although less $40 million in various Alt coins were stolen (and some have already been recovered), the price of bitcoin and other cryptocurrencies plunged by 10% or more.

Efficiency is achieved by the absence of intermediaries and, in most cases, central administrators, resulting in a system that has efficiencies of cost (no middle man to charge a fee) and execution (near instantaneous updating of the ledger and distribution to each participant, although in public blockchains and certain permissioned blockchains the process can take longer).[3]

The blockchain is versatile. It can be, and is already being used both as "public" blockchains and as "permissioned" private blockchains. The distinction is who is allowed to participate in the network, execute the consensus protocol and maintain the shared ledger.

A "public" blockchain is an open sourced program that allows anyone from any location to download the software necessary to connect to the blockchain. Examples include bitcoin and Ethereum. One of the primary drawbacks of a public blockchain is that large scale distributed ledgers require substantial amounts of electric power to fuel the computational requirements of the network. This is because to achieve consensus, each node in the network must resolve a complex cryptographic problem using substantial hardware and electrical resources, in an exercise called a "proof of work."[4]

Public blockchains are by definition open, which means that there is little to no privacy for transactions and no security with respect to information shared among the individual participants in the network, which is open to all. The lack of privacy and security together means that public blockchains have substantial drawbacks in the enterprise context.

Blockchain also can be used in "permissioned" private networks which are reserved to parties who satisfy the requirements to use these networks. Examples include supply-chain and financial networks. The Hyperledger Fabric developed by the Linux Foundation is an example of a "permission" private network that caters to enterprise requirements.

A private blockchain network requires an invitation and must be validated by either a third party or by a set of rules put in place by the administrator. Permissioned networks place restrictions on who is allowed to participate in the network and in particular transactions. The access procedure can vary. A third party may issue licenses for participation; or a consortium of parties may set the rules and make the decisions. Once becoming a party to the blockchain, an entity will participate in maintaining the blockchain as a decentralized system.

---

[3] See discussion in a later blog about the different types of blockchains.

[4] A "proof of work" ("PoW") system or protocol or function is an economic measure used to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. "Mining" of coin is an example of proof of work. See discussion below. A PoW is to be distinguished from a "proof of stake" ("PoS"). PoS is a type of algorithm by which a cryptocurrency blockchain network attempts to achieve consensus. The PoS concept states that a person can mine or validate block transactions according to how many coins that party possesses.

I will discuss how public and permissioned blockchains operate and the present and potential uses of these network systems, as well as hybrid versions of each, in greater detail in future blogs.

What is a Cryptocurrency?

A cryptocurrency is a digital or virtual unit of value, that can be used as a medium of exchange. The defining feature of cryptocurrency is that, unlike fiat currencies, it is a decentralized system that does not depend on any central authority. It uses cryptography to secure and verify transactions as well as to control the creation of new units of a particular cryptocurrency. Essentially, cryptocurrencies are entries in a database that no one can change unless specific conditions are fulfilled.

Cryptocurrency began with the idea of creating a digital currency, separate from a central governmental authority, a peer-to-peer network where holders of digital currency would deal directly with other peers in the network in transactions in the currency. However, without a central authority who would prevent a holder of a digital currency from spending the currency again and again?

Developers of cryptocurrencies struggled with this dilemma for 30 years.

In October 2008, in a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," a person or persons using the pseudonym, Satoshi Nakamoto, proposed a solution: the use of a distributed ledger and tokens of value. This solved the double-spend problem by providing all participants in the network with a record of the transactions. Thus, the network of participants in the ledger validates each transaction by consensus, including the balance of every account. If even one participant in the network disagrees on the validity of the transaction, the transaction fails to become part of the permanent record.

How do cryptocurrencies work? In a typical cryptocurrency transaction, the holder creates a file that says, "Holder A pays X coin to Holder B." Holder A validates the file with her private key (more about this later) and sends the transaction to the network of participants. However, only if the entire network confirms the transaction through its public key is the transaction confirmed. Once confirmed, the transaction is permanent and no longer reversible.

"Miners" perform the job of confirmation. A "miner" can be anyone with access to the internet and suitable hardware possessing the computing power to compile recent transactions in the cryptocurrency. Miners do this by dividing the transactions into blocks and solving a computationally progressively more difficult algorithm. The participant who first solves the algorithm gets to place the next block on the block chain and claim rewards. The rewards are newly released cryptocurrency and often transaction fees, payable in cryptocurrency. The rewards, however, diminish in amount over time as additional cryptocurrency are released and progress is made towards mining the finite number of coins, preset in the code of the

cryptocurrency. The amount of the reward, in coins and transmission fees, are generally predetermined in the code underlying the cryptocurrency.

Bitcoin is the most-well known and traded cryptocurrency. Because of "forks"[5] in the code, it has spawned many variations. But bitcoin is restricted to the currency use case.

However, there are other cryptocurrencies. Of these, the best known is ether. Ether is the unit of cryptocurrency used on the Ethereum blockchain. Unlike bitcoin, it can be used as more than a store of value. Ether permits developers to write their own programs, as "smart contracts" or "autonomous agents," as the Ethereum White paper calls them. The language of Ethereum is "Turing-complete," meaning it supports a broader set of computational instructions.

Among other things, Ethereum smart contracts can:

- Act as "multi-signature accounts," requiring a percentage of parties to the blockchain to agree before funds are spent;
- Manage agreements between users;
- Provide utility to smart contracts; and
- Store information about an application.

One of the primary use cases is to use Ether as a means of buying services within the Ethereum blockchain.

I will discuss Ethereum smart contracts in greater detail as part of my discussion of smart contracts in a later blog.

So Where Do You Keep Your Cryptocurrency?

In a crypto wallet of course! But a digital wallet is quite different from your physical wallet. A digital wallet is a software program that stores your private and public keys, which are used to send and receive coins through the blockchain. Your digital wallet also keeps track of your coin balance.[6]

[5] A "fork" is a split in the blockchain of a cryptocurrency. It can occur in two ways: (1) a fork is caused by a split in consensus that occurs when miners discover the block at the same time, resulting in a temporary fork because as the chain finds the next block this becomes the longest chain and the shorter chain is abandoned by the network; and (2) a fork is caused by a change in the underlying rules of the protocol which occurs when a conscious change is made in the underlying code by the developers and is permanent. Generally, when a fork is discussed, it is the later situation that is meant. Accordingly, forks generally occur because the developers have determined to add new features to enhance the network's functionalities or to change a core rule (such as increasing the block size). Forks can be used to create new cryptocurrencies. I will discuss forks in greater detail in a later blog.

[6] Most coins have an official wallet or a few officially recommended third-party wallets for a particular type of coin. *See, e.g.*, Bitcoinpaperwallet.com; bitaddress.org (examples of paper wallets which provide certain wallet services for free and are generally safe from online hackers); Coinbase/Gemini/Kraken/GDAX/Bitstamp (examples of

Your private keys give you control of the coins you own and must match up with the public keys of the person to whom you send cryptocurrency coins. When you send a cryptocurrency coin, you are sending value in the form of a transaction which transfers ownership of the coin to the recipient.

Your private keys are like your private pass code. If someone finds out your private key code they can access your coins. Also, if you lose your private keys, you lose access to your coins and, unlike in the case of a private pass code, there is no central authority that can provide you with new private keys to allow you to access your coins.

Why not just use the public wallet provided by opening an account with a cryptocurrency exchange? Although this can be done, if you rely on a public wallet administered by a third party you lose control of the private and public keys that control your coins and open yourself to the risk of hacking or a shut-down of the exchange and add a layer of cost and complexity.[7]

In any event, you will need a wallet of some type to trade or hold any cryptocurrency.

Uses

As discussed above, digital ledger technology and the blockchain's ability to enhance exponentially the security and efficiency of commercial relationships will remake the world. It will do this by permitting "trustless" transactions with others. It will allow us to collaborate with other parties without the need for a trusted third-party intermediary. One example is the

---

exchange hosted wallets which accept fiat deposits (U.S. dollars) and exchange services from bitcoin into other cryptocurrencies and fiat currencies (and back again).)

[7] Cryptocurrency exchanges are largely unregulated. However, both the Securities and Exchange Commission (SEC) and the Commodities Futures Trading Commission (CFTC) have suggested that cryptocurrency exchanges should be regulated, at least in some circumstances, under the Securities Exchange Act of 1934, as amended (the Exchange Act), and/or Commodities Exchange Act of 1934, as amended (the CEA).

The cryptocurrency exchange, Kraken, recently stated that they would likely register as a broker-dealer and then as an alternative trading system (ATS). An ATS is a trading venue that operates outside of the traditional public stock exchange system pursuant to Regulation ATS promulgated under the Exchange Act, which provides an exemption from the Exchange Act's requirement that entities that fit the definition of an "exchange" under the Exchange Act must register with the SEC.

The Chicago Board of Exchange (CBOE) became the first major derivative exchange to launch Bitcoin futures in December 2017. Soon after, the Chicago Mercantile Exchange (CME) Group launched its own version of Bitcoin futures trading. Nasdaq plans to begin trading in bitcoin futures before the end of 2018.

In a future blog, I will discuss the regulation of cryptocurrencies and other "cryptocurrency investments" (defined to include derivative products such as options, futures and swaps, as well as cryptocurrency tokens, initial coin offerings (ICOs) and hybrids which are combinations of cryptocurrencies with equity and debt, including debt which is secured by physical assets, as well as the regulation of participants in the cryptocurrency markets.

use of “smart contracts” which allow for the automatic execution of some or all of the terms of a commercial relationship using code embedded into a blockchain digital record.[8]

Future Blogs

My next blog will delve deeper into the use of distributed ledger technology and the blockchain in current and future practice, including the use of the blockchain in business transactions, such as capital formation and financing. I will also discuss regulatory developments, including those applicable to cryptocurrency and initial coin offerings, under the securities, commodities, tax, money transmission and banking laws, as well as those applicable to different market participants utilizing digital ledger technologies and the blockchain. In each blog I will expand upon some of the concepts introduced in this blog, including “smart contracts,” public and private blockchains, “forks” and different types of cryptocurrencies.

[8] Smart contracts will be discussed in greater detail in my next blog.