Blockchain, the Legal World, and Trust

By Mark Belkin

In the world of digital transactions, Blockchain is a technology that will change the concept of trust. It will change the legal profession, banking, trade, supply chain tracking, sales, and almost any industry that has need for recording a transaction. I know a lot of articles claim to be talking about "a technology that is going to change the world!," but Blockchain most certainly will.

Mark Belkin

The most popular application utilizing Blockchain, and the reason it may exist, is Bitcoin. Much has been made of Bitcoin and other cryptocurrencies. This article will touch on it, but will not delve into how these new forms of currency will be regulated, traded, and used. Although questions surrounding the SEC, FEC, BitLicense, and banking laws touch on the monetary and securities issues, this article will focus on Blockchain as a technology, and how the concept could revolutionize the legal, as well as many other, industries.

Basically, a Blockchain is a ledger of records organized into blocks that are linked together by cryptographic validation. It is the digital storage of consensus truth, on a virtual ledger, verified by every computer on the Blockchain network. As the technology grows, the amount of computers using Blockchain increases, and the verification qualities encompassed in the process will gain stronger acceptance. Billions of computers will be used to verify every single transaction. Right now, there are many accepted entities that have a centralized form of verification, such as banks or governmental agencies. Blockchain is de-centralizing that control, and creating a universal networked verification system. Trust is no longer needed, because the system doesn't work unless everyone agrees. Trust becomes a mathematical formula, rather than a malleable entity to be manipulated by interested parties.

Before proceeding forward, I must note that this technology is evolving daily. The landscape is ever-changing and much of the law surrounding the technology lacks precedence. There are issues with transaction speed, scalability, cybersecurity, implantation in industries, and so much more. This article is meant as a layman's brief introduction into a complicated technology—and should be taken as such.

A Look at What the Technology Really Is

Like a traditional ledger, Blockchain is a record of transactions. While most ledgers are centralized (e.g., a database, a book, or an Excel file), this ledger is decentralized and exists everywhere that is connected to the Blockchain. It could be open source, but it's encrypted in a way only a special key will be able to access its information. Every transaction on this ledger can only be executed if it is 100 percent verified by everyone on the chain. These transactions could consist of anything—money, work identification numbers, deeds, your car's history, coffee bag deliveries, pet vaccines—almost anything, that is.

Anytime the information entered into the Blockchain is changed, added, or removed, there is unique marker of that transaction. You can't fly under the radar, you can't hide it, and it is there for everyone to see. Either "everyone" verifies that the transaction occurred, or no one does. Not the government, not your firm, not a corporation, not a credit card company, not your preferred global payments center, but everyone. Everyone has to agree, or the transaction simply did not occur.

How It Works

I'm now going to try to delve into the mechanizations involved. Even though I come from an IT and programming background, it can all seem esoteric to me as well. If you have any questions, feel free to email me.

1. A transaction occurs on the Blockchain, and this puts data into **blocks**. That data is time stamped. When the block has been created, it is (in theory) forever sequential. This avoids anyone or anything claiming to own a duplicate block. To avoid duplication on the micro computing level, the block looks to the longest **chain**. These usually consist of blocks that solved a mathematical algorithm in the fastest time.

2. Once the data is added to the block, it goes out into the **network** and is added to Blockchain. The data is protected by using asymmetric cryptography (a public and private key). **cryptography** is a process in which data is stored and transmitted in a way where only those for whom it is intended can read and process it. You may be most familiar with the process if you've encrypted an e-mail or a form, which many attorneys have done so at least once.

3. Even if multiple transactions are sent at the same time, the time stamp decided by the network ensures that the data will always be in the right order. Everyone on the chain automatically gets updated to the longest (newest) Blockchain.

Mark Belkin, Esq. is currently an Associate Professor at Pratt Institute, and consults with companies on legal and emerging technology matters. He can be reached at markbelkin@gmail.com.

4. The data is turned into a **hash**. The hash is what makes the Blockchain so secure. It is the basis for the cryptography and is the link between blocks. Each hash is unique, and theoretically cannot be duplicated. A hash from one block is a part of the hash of the next block, and this goes on and on and on. A linear chain is created between these blocks, theoretically going into perpetuity, with new ones constantly being created and containing some new information or transaction.

5. If someone changes any of the data in a previous block (cryptocurrency, smart contracts, whatever it might be), the hash alerts the next block that they no longer match. This continues down the block, and since everyone on the chain has the most updated copy, then everyone now sees this change. You can't hide a change. You can't say, "I never did that." It is simply there for the entire chain to see.

6. For particular transactions, like cryptocurrency, the verification process is done through **digital signatures**. When a transaction occurs, every **node** (computer) on the chain checks the digital signature for authenticity. Only when authenticated by every node does the transaction proceed. These digital signatures are mathematical algorithms designed specifically to prevent copying or forgery. The digital signature consists of a private key, which you should not share, and a **public key**, which is what you share to allow a transaction to occur. The public key is the address you use to accept the transaction, and may be referred to as a **Wallet**.

Steps in a Typical Transaction—From the User's Perspective

1. When users execute a transaction/contract/purchase, they are given a string of data called an **address**. Addresses are added to the Blockchain as soon as they are used in a transaction and anyone can see them.

2. For each address, users are given a **private key** which must be used for the transaction associated with that address. Transactions could include payments, private information, or data. The private key is what is used to authenticate the owner of this transaction. DO NOT LOSE THIS KEY. Once lost, funds in that address are locked forever. There are cases where people have lost millions of dollars because of lost or destroyed private keys.

3. A new private key is created after every transaction, and a new address is assigned to the user. The address is what allows others to know that every new transaction is authentic. It is also possible to do the transaction from an existing address using a **signature**. The signature is generated using the private key, and can be used to prove that you are the owner of the key, without having to reveal that private key itself.

Digital Identif cation

The loss of privacy makes the ability to safely store information as imperative as it has ever been in our modern society. A secure mechanism capable of protecting data—all types of data—could revolutionize industries that require forms of identification. Government-issued IDs are not foolproof against counterfeiting or theft. In an increasingly globalized business and legal environment, people are looking for the evolution of simplified yet verifiable authentication. Blockchain could allow individuals or groups to easily prove their identity. Imagine entering a corporate office in Shanghai, China with the same identification you used in the office of a completely different corporation located in Austin, Texas. However, it would be equally secure, and could potentially store anything necessary for that particular meeting or transaction. As long as they are verified within the parameters of a classification, you can trust that person is who they say they are.

It might seem frightening, but anything that could be digitized—including someone's fingerprints, eye scans, signature, name, blood type, medical history, and security clearance—can be stored in this kind of identification. This Universal ID then might be used anywhere in the world, with absolute trust in verification capabilities of billions of nodes on the Blockchain network.

What Is a Smart Contract?

Smart contracts are a set of code that executes a transaction if certain parameters are met. **If** a certain condition occurs, **then** the smart contract executes. You could use smart contracts to transfer anything of value, like cryptocurrency, real estate, assets, life insurance, medical bills, car purchase history, etc. Smart contracts can connect multiple Blockchains, using encrypted digital signatures from a seller and buyer, thereby verifying the conditions necessary to execute and then executing the transaction. Once again, every node must verify every transaction that is on the Blockchain.

Imagine the implications of 100 percent verifiable transactions verified by billions of "witnesses" (the nodes on the Blockchain), when enforcing judgments, carrying through financial transactions, working with

escrows, sharing judicial orders, and so on. The terms of the contract are encoded on a shared ledger. No one can say, "I lost the contract." They may lose the private key, but the terms of the contract execute no matter what. As the Blockchain grows, the ability for people to back out of their obligations will become increasingly difficult. Like most industries, this will signal a paradigm shift for the legal industry and eventually attorneys will need to adapt to this new technology.

Cybersecurity

Hacking is something that everyone is concerned with these days. This is no different with the Blockchain. No matter what protections are created, there is some innovator in a basement somewhere finding a crack to that code. Already a few cryptocurrecy platforms have been hacked, and people have lost insane amounts of money. This is something that is still being worked out, and the growing pains will be substantial.

Further Questions

- How will regulators respond to the newfound transparency?
- How do federal and worldwide securities regulators react to an ever changing new form of currency?
- How will governments respond to the loss of some centralized powers?
- How will liability, breach of contracts, and other legal issues be resolved by legislators and common law?
- How will the technology change the role of lawyers?
- How long before it can be implemented in different industries?
- How can those using the technology be promised they will be protected from hackers and other bad actors?

These are some of the many questions that will keep countless attorneys and industries away from implementing the technology in the short term. However, much like the internet, databases, and digital documents, it is only a matter time before the underlying concepts and technology of Blockchain will go mainstream and change the world.

I want to acknowledge the website blockgeeks.com for much of my information.

Like what you're reading?
To regularly receive issues of *Inside*,
join NYSBA's Corporate Counsel Section
(attorneys and law students only).