

Blockchain: Cryptocurrency foundation and the future of information management and security

By Marc S. Voses, Esq., and Jeffrey S. Matty, Esq., *Kaufman Dolowich & Voluck**

JULY 27, 2018

Bitcoin burst upon the scene in 2017, shining the light on a payment methodology that would spawn the birth of hundreds of new cryptocurrencies. By mid-2018, there would be close to 1,600 with a total market cap of over \$250 billion.

While blockchain technology has become popularly known for being the backbone of cryptocurrencies, it also serves as the foundation for protocols that will manage and secure a broad spectrum of information in the near future. This expert analysis explores some emerging issues concerning cryptocurrencies and the fascinating new potential for storing and securing data.

BLOCKCHAIN: A PRIMER

Imagine you are in the possession of important information. If you place that information on a ledger (a document containing a host of information) and place the ledger in a box, you can verify the information contained on that ledger by opening the box and examining the details — and so can anyone with whom you share the ledger.

The information contained on the ledger, however, can be verified only at the time of the examination; if you make a change, it is no longer the same information that you or anyone else previously verified.

What if you scan the ledger and place it in a folder on your computer server? Again, you can verify the information contained in the folder, and you can allow others to remotely view and confirm it.

However, this method suffers from the same limitation as the ledger in the box: It can be altered after being verified, and no one would know unless you check the ledger again.

Now, imagine you have a network of individuals who want to share information with each other. Each has a computer server (called a “node”) that can access the network. You are the first in the group to upload the information discussed above to a spot (a “block”) on your network’s electronic ledger. Because your block is the first on the ledger, it will be referred to as the “genesis block.”

After you upload your information, it is copied to the network ledger. Each node has a copy of the ledger and compares its copy of your block to the block contained on the ledger maintained by every other node in the network. If the nodes all agree that they all

have the same copy of your block, it is time-stamped, frozen, made unalterable and permanently recorded as a block on the ledger.

When someone else on the network wants to upload information to a block on the ledger, the same process will be followed. Their block will be permanently linked to your block, and so on and so forth, creating a chain of blocks — hence the term “blockchain.”

Every node in the network has access to the information contained in the blocks that make up the blockchain. This is why it is referred to as a “distributed ledger.” Each block is identified by a unique digital signature that locks in the information contained in the block, and it is periodically checked against every other ledger in the network for consistency. This is why it is considered immutable.

Blockchain technology not only serves
as the engine for cryptocurrencies; it also advances
the digital management of information.

If a change is detected in a block on a ledger maintained by a node, that block is removed from the blockchain and replaced with the information contained on the other nodes. While this is an oversimplification of the process that blockchain enables, it gives an insight into the power of this technology.

CRYPTOCURRENCIES: THE ALLURE OF MINING BITCOIN

Bitcoin is a cryptocurrency built on blockchain technology. The difference between the data storage example above and a cryptocurrency is the protocol, or rule, that governs the manner in which block is created and its operational purpose. The bitcoin protocol requires network nodes to complete complex mathematical formulas, a process called “mining.”

Once a node’s mining efforts solve a designated mathematical formula, its proof of work is distributed to the other nodes. The other nodes then examine whether the node has properly solved the formula.

Assuming the node’s proof of work is correct, the hard work of mining is rewarded with possession of a block on the bitcoin blockchain. As with the information example above, each bitcoin block has a unique serial number identifying it on the distributed ledger.

This process continues at a rate that is regulated by the bitcoin protocol. The controlled creation of bitcoin assures its scarcity and creates an intrinsic value. Each new bitcoin block is joined to the prior block, creating a chain that is secure and known to all who possess a copy of the ledger.

Bitcoin is the most popular of all cryptocurrencies. After languishing in relative obscurity for more than five years, bitcoin soared in 2017. It gained international recognition when its market value surpassed \$1,000 per coin, thereafter rising to \$20,000 in December, only to fall back to \$13,000 by the close of the year.

The astounding increase in bitcoin's value spawned the creation of myriad new cryptocurrencies and other blockchain-based protocols, creating an environment that has drawn the attention of those seeking to capitalize on this new technology for both legitimate and less scrupulous purposes.

CRYPTOCURRENCY FAILS AND HOPE

Like those athletes on YouTube attempting death-defying feats only to land face-first on the pavement, some people seeking to replicate bitcoin's success have achieved less than spectacular results.

Take for example the case of REcoin, whose founder, Maksim Zaslavskiy, is now a defendant in both a criminal case brought by the Justice Department and a civil suit brought against him and his companies by the Securities and Exchange Commission for selling unregistered securities.

REcoin and Diamond were touted as the first ever cryptocurrencies backed by real estate and physical diamonds, respectively. Unlike bitcoin, which relies on the public to set its price, the value of REcoin and Diamond would be set by those hard assets.

The founders of REcoin and Diamond sought to raise capital using an initial coin offering, whereby those who subscribed would be issued REcoin and Diamond "coins" in exchange for their investment.

The U.S. Attorney's Office for the Eastern District of New York described the problem with these two ICOs as follows:

Virtual currency, such as that promoted in these ICOs, is a digital representation of value that can be digitally traded but does not have legal tender status, and functions only by agreement with the community of users of that particular currency. Zaslavskiy and his cohorts promised substantial returns to investors even though neither company had any real operations. With respect to REcoin, Zaslavskiy advertised that the company had a "team of lawyers, professionals, brokers and accountants" who would invest the proceeds from the REcoin ICO into real estate when in fact no such employees

had ever been hired or even consulted, and no real estate investments were made. Similarly, Zaslavskiy told prospective investors in Diamond that their investment in Diamond tokens was "hedged by physical diamonds," even though Diamond had not actually purchased any diamonds or engaged in any business operations.¹

This is just one of a number of criminal and civil complaints filed against those that seek to profit through the issuance of an ICO.²

It has become clear that blockchain startups are struggling to legitimately negotiate an uncharted path toward completing a successful ICO.

One startup, Prometheus, is planning to raise up to \$50 million through its ICO and says its path to success is complying with Regulation A+, which the SEC adopted to help smaller companies raise capital. Whether that course is the appropriate way to achieve a legally compliant ICO remains to be seen.

Watching this new technology emerge on the scene has been just as interesting as witnessing the creation of its accompanying regulatory framework.

BLOCKCHAIN: PROTOCOLS FOR THE AUTHENTICATION AND SECURITY OF INFORMATION

Blockchain technology not only serves as the engine for cryptocurrencies; it also advances the digital management of information. This new technology is expected to streamline the purchase and sale of assets, and it will also serve to verify ownership rights to those assets. These are just two of the many functions that blockchain technology will facilitate and simplify.

Take for example a real estate transaction. Hours are spent locating and verifying information that is needed to close the deal. As part of the process, numerous pieces of information – including the deed, title insurance, water and electric bills, satisfaction of prior mortgages, clearance of violations, a property survey, certificate of occupancy, property taxes, insurance, and the identities of the seller and purchaser – must be found and verified as accurate, often by a team of highly qualified (and expensive) attorneys. Blockchain has the potential to shorten this process and reduce costs.

Protocols are being created that will link all the pieces of information associated with a sale of real property.

Here is an example of the information that could be linked together in a distributed ledger that could not be altered:

- Survey
- Deed
- Mortgage
- Mortgage payment

- Insurance
- Property taxes
- Notice of nonpayment of property taxes
- Construction permit
- Water bill
- Electric bill
- Gas bill
- Building code violations
- Satisfaction of violations
- Certificate of occupancy
- Cancellation of insurance for nonpayment
- Reinstatement of insurance
- Property tax lien
- Satisfaction of property tax lien
- Satisfaction of mortgage
- Transfer of water bill to new payer
- Transfer of electric bill to new payer
- Transfer of gas bill to new payer
- New deed following sale to new owner(s)

A blockchain protocol that links together all these aspects of a real property transaction could provide immediate, authentic and verifiable information establishing legal ownership of the property and any liens or encumbrances affecting it.

Interestingly, Kenya is moving forward with a plan to use blockchain as a means of addressing land ownership disputes, creating a system that is verifiable and reliable.

Blockchain technology is also already being used to track meat, produce and ingredients used in food throughout the chain of commerce. Consumers would be given access to a whole host of verifiable information concerning their food, such as whether it is organic, where it was grown, when it was picked, what certain animals were fed, and how that food product was transported and under what conditions.

It could also speed the identification and notification of people who purchased food that is discovered to be potentially contaminated, improving responses to product issues, making the dissemination of product recall information more efficient and, most critically, saving lives in the process.

CONCLUSION

In closing, we are reminded of a quote by R. Buckminster Fuller, who was, among other things, an inventor and futurist: "You never change things by fighting the existing reality.

To change something, build a new model that makes the existing model obsolete."

Blockchain has already given rise to payment methods that serve as alternatives to traditional fiat currency. It is also starting to revolutionize data security and information sharing, giving rise to countless benefits that will reduce transaction costs, provide greater transparency and foster trust.

While this new technology will be manipulated by fraudsters and may result in the elimination of certain functions within specific industries, blockchain may just be that new model that makes existing models obsolete.

NOTES

¹ Press Release, U.S. Dep't of Justice, Brooklyn Businessman Charged with Fraud in Connection With Two Initial Coin Offerings (Nov. 1, 2017), <https://bit.ly/2zqYaT9>.

² See *SEC v. PlexCorps et al.*, No. 17-cv-7007 (E.D.N.Y.); *SEC v. Titanium Blockchain Infrastructure Servs. Inc. et al.*, No. 18-cv-4315 (C.D. Cal.); *SEC v. Sohrab et al.*, No. 18-cv-2909 (S.D.N.Y.); *CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018); see also *CFTC v. My Big Coin Pay Inc. et al.*, No. 18-cv-10077 (D. Mass.); *U.S. v. Trapani*, No. 18-mg-3271 (S.D.N.Y.); *SEC v. Sharma et al.*, No. 18-cv-2909 (S.D.N.Y.); *U.S. v. Sharma et al.*, No. 18-mj-2695 (S.D.N.Y.); *SEC v. AriseBank et al.*, No. 18-cv-186 (N.D. Tex.).

This article first appeared in the July 27, 2018, edition of Westlaw Journal Computer & Internet.

* © 2018 Marc S. Voses, Esq., and Jeffrey S. Matty, Esq., Kaufman Dolowich & Voluck

ABOUT THE AUTHORS



Marc S. Voses (L) is a partner and co-chair of the data privacy and technology services practice group and the insurance coverage and litigation practice group at **Kaufman Dolowich & Voluck** in New York. **Jeffrey S. Matty** (R) is a partner at the firm. His practice focuses on complex coverage matters for domestic and international insurers.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.