LAWRENCE, EVANS & CO.,LLC

Investment Banking | Corporate Finance | Consulting

BLOCKCHAIN IN HEALTHCARE

Whitepaper

November 2018

Table of Contents

Section: Page:

Blockchain in Healthcare Introduction

Blockchain is seeing great success in the financial industry, and is being investigated to great lengths as to how it can be used in the healthcare industry. Healthcare inefficiencies, whether supply chain, claims data and records management, or revenue cycle and the need for transparency and security, are a perfect fit for the technological capabilities of blockchain. In healthcare, maintaining security of Protected Health Information (PHI) is paramount. The Health Insurance Portability and Accountability Act (HIPAA) required particular identifiers such as names, social security numbers, etc. be treated with special care. This increased emphasis on security requires those handling PHI to take extra precaution.

Even after taking extreme care, there exist many threats, internal and external, to the security of health records and hospitals are under constant threat of hacking/phishing attempts. For example: the accidental downloading of malicious software can infect an entire hospital's IT infrastructure and compromise PHI. In 2017, Erie County Medical Center was taken down for a six weeks, making it difficult for patients to seek care as physicians had trouble accessing medical records. Hancock Regional Hospital in 2018 was held hostage with SamSam Ransomware, leaving its systems temporarily disabled. The hackers were successful after Hancock paid the hackers $55,000 worth of Bitcoin before obtaining a decryption key and unlocking their systems. Hackers have great incentive to steal health records as such information can be sold on the black market. According to CBS News, hackers can sell credit card records for between 10 and 15 cents each, but a medical record can sell for $30 and possibly up to $500.

Blockchain has the potential to allow for a copy of the hospital's records to be shared amongst many computers, even ones that are not directly infected by the virus. Therefore, the blockchain could help prevent hackers from compromising a hospital's database. Although EHR is just one of many implementations of the blockchain, this paper dives into what blockchain is, where it is practical, and some projects that are currently implementing it.

SamSam Ransomware
Source: malwarebytes

What is a Blockchain?

Over the past few months, there has been a lot of hype around the word "blockchain," leading to a great divide in companies looking to leverage the buzzword for marketing, and others publishing genuine thought leadership. Frequently, the word "decentralized" may be used as one of the main buzzwords associated with blockchain. Even that is tossed around a little loosely, as different implementations of the blockchain provide for different magnitudes of decentralization. Another big misconception is that a blockchain must have some sort of crypto "asset" such as Bitcoin or Ethereum associated with it. We discuss later on that only a handful of implementations actually have such crypto "asset" associated with it.

So what is the blockchain? The "blockchain" is a ledger of encrypted data that is copied amongst all participants (or nodes) in the network. You can think of it like an Excel spreadsheet or Google shared files. Imagine that you and your colleagues are working on the same spreadsheet, adding new rows containing unique information. The computer you are working on represents a "node," which will be used to verify yours and others' changes

to the spreadsheet. When you click save on your spreadsheet, it sends the changes out to the other excel workbooks in an encrypted fashion.

For them to accept the changes, there needs to be "consensus" amongst the nodes that you are, in fact, a participant in the network who is authorized to make changes. How consensus is done varies depending on what blockchain type is used, but the general principle that everybody now has an updated copy of the excel spreadsheet is the same across all types. Once consensus is reached, everyone's updated copy is reflected across all nodes, and the thus the size of the blockchain has increased as well. We will touch on why this can be problematic later.

In a sense, you can think of the blockchain as an encrypted database. Additionally, the database is shared amongst "nodes" or participants in the blockchain network. Consensus process differences are another important learning block to understanding the blockchain. In layman's terms, how do other blockchain participants determine what changes to the blockchain are legitimate and which ones are illegitimate. In a public blockchain, anyone can participate. Anybody's tech savvy child can turn their computer into a mining rig. Therefore, blockchain must use creative ways to prevent the blockchain from being falsely modified. This is done through Proof of Work (PoW) and Proof of Stake (PoS), which we will touch on later. In a private or consortium, all the participants (nodes) are already known, so there is no need to require PoW or PoS consensus mechanisms. Instead, consensus is gained from the simple fact that other nodes recognize that the changes made were made by a permissioned participant.

Glossary

Ledger – a copy of the information that is shared amongst nodes, much like an excel spreadsheet

Node –a computer, often more powerful than a regular PC, carrying a copy of the blockchain ledger and participating in the consensus process (sometimes referred to as participants)

Consensus – the method by which the blockchain uses to verify a new data entry to the blockchain

Miner – a node in a public blockchain that uses the Proof of Work or Proof of Stake consensus method to agree on a change

Decentralization – the nature of the blockchain being shared amongst many single nodes

Benefits of a Blockchain

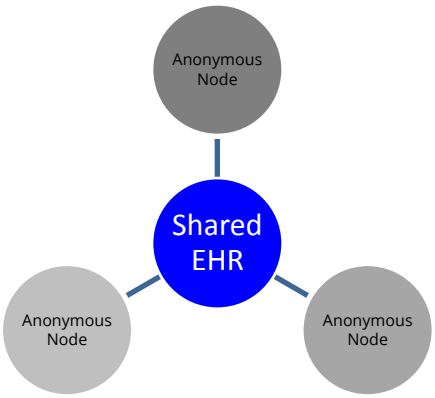
The primary advantages that are gained from blockchain are that of security and trust. Because every node in the blockchain must have the exact same copy of the ledger, every change to it is transparent and clear to every participant. Therefore, there is a sense of trust amongst the participants in the network. This concept could be important for the use of financial institutions when verifying transfers of money and preventing fraud. In the healthcare industry, the blockchain could be used for claims processing. For example, practices could be deterred from billing for services they did not provide, as the ledger could be permanent and audited back to the beginning of time.

Along with trust comes the added layer of security. In healthcare, interoperability and security are of the upmost importance. Exchanging healthcare information amongst the required parties requires extreme care. The blockchain, if implemented properly, could provide a safe exchange of information, as only verified participants can have access to such information.

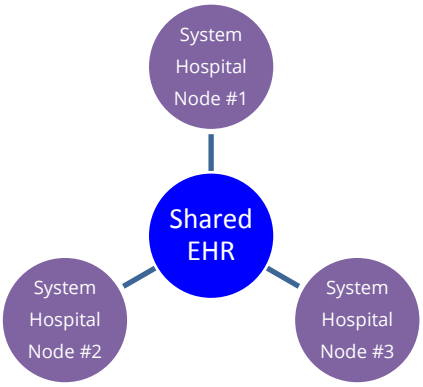
BLOCKCHAIN TYPES

There are three types of blockchain database applications that can be made: Public, Private and Consortium. Each of them have their own respective advantages and disadvantages.

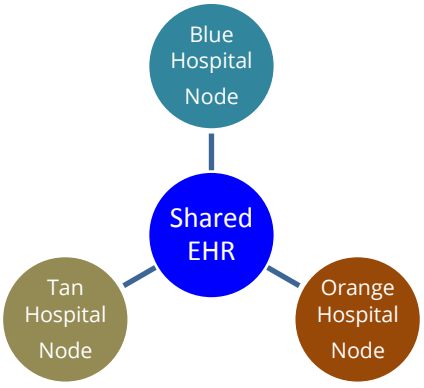
Public Blockchain: A public blockchain involves countless nodes that can participate from anywhere in the world. Anyone can read the blockchain and help verify if transactions are valid. This type of blockchain is completely decentralized, meaning nobody is a single owner of the blockchain. In order to incentivize nodes to participate in the blockchain, they will often be rewarded with some type of crypto-coin. In the case of the Bitcoin blockchain, participants are offered a part or whole of a Bitcoin as a reward. A node can be interpreted as a "*miner*" in the case of a public blockchain – a computer with high-powered Graphics Processing Units (GPU). Because of the completely decentralized nature, confirming a change to the blockchain ledger amongst nodes takes much longer than a private or consortium blockchain would. Therefore, for a public blockchain, you sacrifice speed and efficiency for decentralization.



Private Blockchain: A private blockchain is one where the reading and writing is all done by one central organization. The private blockchain has a predetermined number of nodes, each of which works with each other to determine consensus to changes in the blockchain. Additionally, it is somewhat decentralized, meaning one company such as a hospital network (example shown with 3 hospitals) can have nodes across many of its facilities, but it generally would not extend to other companies (otherwise it would be a consortium).



Consortium Blockchain: A consortium blockchain is one where a predetermined number of nodes verify changes to the ledger. Unlike the private blockchain, the consortium blockchain is shared amongst a group that has similar desires in accessing the information. This may be used in applications where a slight decentralization would be good for security, but complete decentralization would not make sense. To imagine an application of this, think of voting. Voting machines could verify amongst each other when votes are added so that the chain is expanded on, but no third party system could manipulate the votes. In healthcare, this could be similar to a HIE where a group of hospitals or health providers share information.



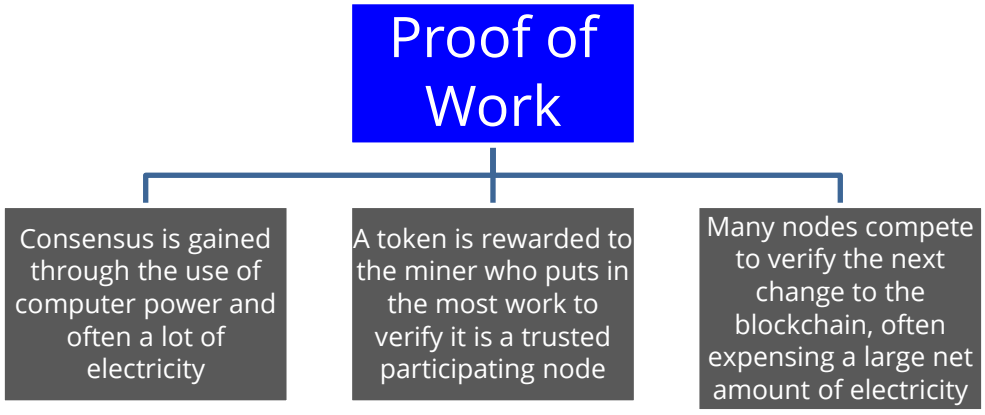
Blockchain Types

	Public	Private	Consortium
Access	Open reading/writing	Permissioned Participants Only	Permissioned Participants Only
Speed	Slowest	Very Fast	Fast
Consensus	Proof of Work & Proof of Stake	Predetermined Participants	Predetermined Participants
Node Identities	Anymous	Known	Known

PUBLIC BLOCKCHAINS

When people generally think of blockchain, they usually think of characteristics of a public blockchain such as crypto tokens. This is only one method of implementing the blockchain, however. Public blockchains are open, meaning that any single person can create a node for the blockchain, read information on the blockchain, and write information to it. So, how then would the blockchain prevent a malicious node from manipulating the chain? The blockchain can do this through *Proof of Work* or *Proof of Stake*.

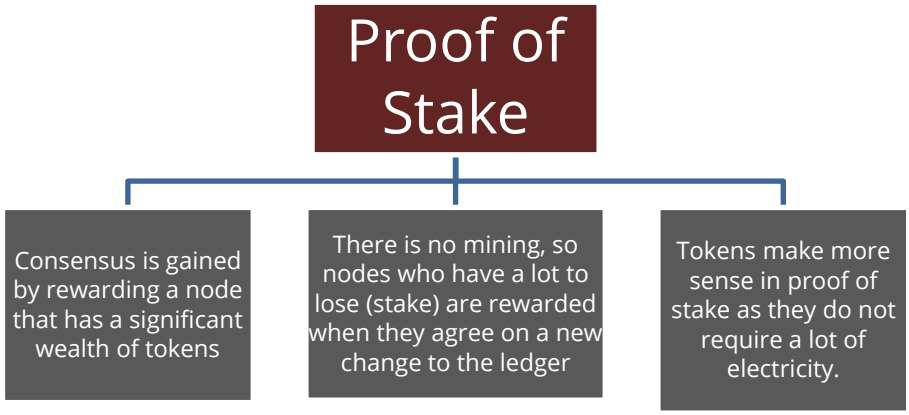
Proof of Work – In a public blockchain, there needs to be an incentive to reward good actors and punish bad actors. This can be done through Proof of Work (PoW). The general idea is that many nodes compete to verify a change in the blockchain ledger and gain consensus in exchange for some sort of crypto token as a reward. PoW requires a large amount of computer processing power, and thus electricity. This means that "mining" a new block can be a very expensive process, even for the miners that are not rewarded. Thus, a public blockchain on the PoW method can be very costly and inefficient.



Proof of Stake – Proof of Stake (PoS) differs from Proof of Work in that it rewards those who are competing for consensus that have the most tokens, thus a larger stake. Therefore, if I have 100 Ether and someone else competing has 10, it's going to reward me with the next mined Ether, as I have more to lose than the guy with 10. In the hospital industry, imagine a shared EMR system with a public blockchain. If a physician were to add changes to a patient's EMR, the node with the most of whatever token was being used on the network would be the one with consensus to verify the change to the blockchain. Therefore, a hacker could obtain a majority of the tokens on an EMR blockchain and add new medical diagnoses for patients that are falsified, or flood the blockchain with fake information scaling up its size and

bogging down the blockchain.

As a result of using high amounts of electricity through PoW or having a pile of tokens for PoS, a public blockchain will reward participants using a sort of crypto token. In the Bitcoin blockchain, that token is Bitcoin. This idea of rewarding nodes for participating in the consensus process with tokens is known as crypto economics. In short, in order to incentivize people, there must be a reward. In this case, the exchange is using processing power (in the case of PoW) or having a large preexisting pile of tokens (in the case of PoS) for a crypto token.



In some cases, the public blockchain network in question will reward a token in hopes that it can become a sort of exchangeable currency, like Bitcoin. There are many projects that offer a token where the creators assume that the value of the token is pegged to the value of the product being created. As we will discuss later, crypto economics is something that has a few fundamental issues.

Private Blockchains

A private blockchain differs greatly from a public blockchain in that it does not require any sort of crypto economics, and it has a set of predetermined nodes that work together to reach consensus. This would be implemented internally within an organization to add an additional layer of security. It is very much like a regular database, except the decentralization across many internal servers (nodes) provides for the added layer of security and trust. A healthcare provider may use a private blockchain in order to keep track of services they've provided and billed for back until day one. That can help keep a long and secure ledger of every transaction that has occurred within a provider.

Consortium Blockchains

One of the most interesting implementations of the blockchain comes through a consortium. A consortium occurs when a few organizations or groups who benefit off the exchange of information with each other decide to all provide nodes for a blockchain based information exchange. Imagine that three different hospitals all agreed that it would be beneficial to be able to access patient records across each other's medical facilities. Each of them may setup 4 nodes, all of which communicate with each other using the security of the blockchain. Like the private blockchain, all participants already know who is a legitimate player and who is not. Therefore, there is no need for costly Proof of Work or Proof of Stake methods for verifying participants. The only downside to the consortium solution when it comes to interoperability is that the ledger can only get larger and larger. There are ways around this, however, with regards to knowing what information must be stored on a blockchain and what does not have to be. We discuss more about this in the next section.

Public Blockchains

The question of practicality really comes down to what type of blockchain is used. A public blockchain is great for trust and security, but is also faced with high costs of electricity if Proof of Work is used. Additionally, crypto economics, the idea of incentivizing people to offer up nodes to participate, has its own issues as well. These issues come in the form of high costs to obtain tokens, and the economics behind crypto assets are hard to rationalize.

The high costs associated with the public blockchain come with the high costs from the consensus processes in Proof of Work. As we have discussed, public PoW blockchains require a lot of energy in order to prevent a bad actor from manipulating it. Thus, many who are using large facilities to mine crypto currencies must hope that the value of the rewarded token exceeds the cost of the electricity. If not, then people will stop mining making it so that the blockchain is easier to hack, as consensus will not require much processing power.

The additional issue with public blockchains is that the idea of crypto economics is a little tough to rationalize under a public blockchain.

The tokens that are used by any sort of blockchain are very similar to "company scrips", or currency issued by companies that can be used to purchase goods and services that the company offers.

Company Scrip
Source: Renolds Stone New York

In Mexico, Walmart employees at one time were paid in part by scrips, which would only be redeemable at Walmart. In other words, Walmart employees were forced in part to use part of their paycheck to shop at Walmart. Walmart eventually lost a case to the highest court in Mexico in which they ruled that Walmart must cease paying employees in part with vouchers redeemable only at Walmart stores. The reasoning behind this is clear. When you are forced to buy products that a company offers, they create a monopoly on that good and therefore are able to mark it up.

In a blockchain token economy, the same concept is true. In order to acquire tokens to access information on the blockchain, say healthcare EMR, one has to gain tokens from either being a participating node in the blockchain, or purchase such tokens from a token exchange. In the case of a node, electricity from running the node is an added expense for obtaining the token in PoW. If you purchase the token on an exchange, it is likely that a fee will be paid in order to purchase it.

Think about visiting France, for example. Let us assume that you lost your iPhone on the way there from the United States, and are in need of buying a new one in order to keep in contact with your travel group. You visit the Apple store and see that an iPhone costs €440, which is equivalent to $500 at the time of this publication. That makes sense, as an iPhone in the United States costs you $500. However, because you are only carrying dollars, you need to exchange dollars for Euros. Exchange rates for Visa are 2-3%, so when purchasing the iPhone, you are paying an additional $10.

Imagine doing that for pull requests of hundreds of medical records per day. Immediately, that extra $10 will continue to add up to a point where it might not make economic sense to have the medical records stored on the

blockchain.

Of course, this could all be solved if the EHR company cut out the exchange and sold tokens directly to the providers to purchase access to medical records. While this is possible, it can also create an unneeded workload on the provider's accounting and finance professionals. Instead of keeping track of the flat-rate paid per month for using Cerner, for example, they will have to keep close attention to the monthly cost differences of paying directly for the medical records on a variable cost versus paying a fixed monthly cost. Additionally, accountants will have to keep track of the inventory of tokens to purchase access to the medical records, and make sure that the hospital will not run out at any given point. Altogether, one may question if these extra costs are worth it.

Other problems arise when discussing scalability. When looking at a public blockchain, each node carries a copy of the blockchain, and each node is powered by electricity. That means that as the blockchain grows larger and cannot decrease in size, nodes will require more storage hardware for the large blockchain, and the net electricity expensed from the entire blockchain will be immense.

Private Blockchains Even private blockchains face some scrutiny with regard to their practicality. Professor Arvind Narayanan of Stanford University argues that private blockchains are just another name for an SQL database. After all, they are just another way for storing information. Furthermore, if the SQL database gets too large, obsolete records can be deleted which is a big advantage over the blockchain. Gideon Greenspan of Multichain argues differently, saying that private blockchains allow for more robustness in that the digital ledger. This is because it can be traced back to day one, and the ledger is copied amongst multiple nodes in a more secure way.

Consortium Blockchains
There seems to be a very reasonable implementation of the blockchain when discussing a consortium if implemented properly. For example, imagine that a hospital system ran a consortium with all of their hospital locations, where at each location they had a few nodes setup to allow for the exchange of healthcare records across all hospitals. That would allow for the safe exchange of information, would not require any tokens in order to access the information, and would allow for an additional layer of security. The only concern would be that the ledger of healthcare records would get too large. In order to avoid this, they could use a partial blockchain, storing only information as to where to access the information, and an access key to access such information.

HEALTHCARE BLOCKCHAIN IMPLEMENTATIONS

Blockchain has the ability to solve a variety of problems in the healthcare industry, mostly with regards to the sharing of data across healthcare providers. During 2017, money began pouring into blockchain projects as people began purchasing crypto assets through Initial Coin Offerings ("ICOs") which were available to non-accredited investors.

In healthcare, blockchain has the ability to disrupt a variety of industries in which information exchange is not only valuable, but there is a need to protect the exchanged information. Blockchain in healthcare is still in its early days, yet we can see some areas where it may be implemented based on the nature of the technology.

SHARING PROVIDER INFORMATION

Centers for Medicare and Medicaid Services ("CMS") punish insurers who do not have up-to-date provider information with a fine. Therefore, it is imperative that insurers have current information on providers. One way

that this could be done, and that all insurers could avoid penalties, is for insurers to share provider information.

Humana, Multiplan, Optum, Quest Diagnostics, and UnitedHealthcare

The combination of these companies have teamed up to create a consortium in which they will create a directory of healthcare providers that they will all work together to keep up-to-date. According to Quest Diagnostics, over $2.1 billion is spent annually chasing provider data. This allows insurers to cut some costs with regard to unnecessary fines.

Of course, one might question whether or not a blockchain solution is necessary for this. Why not use a shared database? Information shared about providers is sensitive, and the cryptographic nature of the blockchain allows for that information to be kept secret except to those who have the private key.

PHARMACEUTICAL SUPPLY CHAIN REGULATION

The Drug Supply Chain Security Act (DSCSA) of 2017 has required that pharmaceutical supply chain participants share information that allows each participant to track a drug from any moment in the supply chain by 2023. This is a great opportunity for the blockchain, as the legislation asks for the technology that is right in blockchain's wheelhouse. Still, it will face the problem of scalability, which could be problematic later on as the blockchain becomes large in size.

MediLedger

MediLedger was created in 2017 after the Drug Supply Chain Security Act (DSCSA) was passed. The company is looking to leverage this legislation and introduce the blockchain as a solution to the new legal requirement. In doing so, the company provides a ledger that allows any participant in the drug supply chain to see when and where a drug was at any particular point in time. This is exactly what the law requires, making it a great answer the new legal environment. The project will use a consortium amongst all participants in the supply chain. Likewise, they have developed partnerships with McKesson, Gentech, AmerisourceBergen, and Pfizer.

CREDENTIALING

One barrier that currently exists in the industry regards credentialing. Today, any time that a physician goes to a different institution, they have to go through a new credentialing process. This can take a long time, sometimes up to three months. Therefore, providing an easy way for physicians to prove that they are licensed to practice in a particular area would allow physicians to get to work much quicker.

Hashed Health

Hashed Health is currently working on a variety of consortium blockchain projects to solve problems that currently exist within the healthcare industry. One of those regards physician credentialing. The solution would be a blockchain that would store the credentials of all practicing physicians in the United States into one location. Physicians would then have the ability to give institutions access to their credentials if they were to give their private key to the institutions, which could be as simple as a QR code that the institution would scan.

MEDICAL RECORD INTEROPERABILITY

Imagine going to one hospital and getting diagnosed with a chronic disease. Now, imagine that you wish to get treatment at a different hospital. When you go to the new hospital and ask them to pull up your records and information on drugs you have been prescribed, it is likely that they will not be able to. Hospitals often do not share medical records amongst hospitals. The blockchain, after solving for scalability issues, could be perfect for this.

MedRec

MedRec is a private blockchain project that is being developed at MIT and lead by Dr. Andrew Lippman, a renowned research scientist. MedRec is designed to allow healthcare providers to securely share EHR for access to patient health records. Instead of storing all of the health records on a blockchain, it uses smart contracts to point to the location of EHR and authenticate that the person trying to reach the EHR is authorized to do so.

MedRec's justification for avoiding a public blockchain and using a private one is important in understanding why public blockchains are not a good solution when it comes to EHR. A private blockchain guarantees that only registered healthcare providers are allowed to make changes to the MedRec blockchain.

Additionally, the project had sought to allow medical researchers to participate by providing a node in exchange for access to anonymous health information. Although not a traditional form of crypto economics, providing data in exchange for a node could be a much better way to incentivize participants.

MedRec could currently be the most practical application of the blockchain to date. However, even the project's leader, after reaching out to him, suggested that the architecture has gone through many changes, and that some of their ideas from the first iteration tend to be much more difficult than they had anticipated.

DokChain by PokitDok

DokChain by PokitDok is private blockchain designed for clinical data and financial transactions in the healthcare industry. DokChain in some ways uses a crypto-economics platform, but not in your traditional sense. Instead, tokens are exchanged internally in the network for medical records and financial transactions. The difference between this

and a public blockchain is that the tokens are not exchanged outside of the network, but are used internally in order to identify legitimate players. Much like MedRec, DokChain uses a consortium in order to limit the amount of nodes who have access to sensitive data. However, the tokens are used to add another layer of security, because in order to get access to data, you must have those tokens, and only such nodes can have those tokens.

Ventech Solutions

Ventech Solutions is an IT solutions company that operates in the healthcare and defense industries. Ventech is currently working on a blockchain consortium solution for both accessing medical records at any provider at any time, and for tracking claims from provider to payer.

The company uses an on-chain off-chain strategy. Instead of storing medical record information all on the blockchain, they only store important information on the blockchain such as where to access the health records. That way, the blockchain will not scale with bulky and unnecessary information.

CONCLUSION

Blockchain has the potential for information to be shared securely amongst trusted parties, which is perfect for areas in healthcare where interoperability is important. While we are seeing companies invest into blockchain projects where there could be uses such as drug supply chain, medical record interoperability, credentialing, and sharing provider information, it has yet to be seen whether or not blockchain will be successful in these areas.

At this point in time, it is difficult to determine if public blockchain projects will make it to the spotlight in healthcare. Because of the open nature of the blockchain, there remains the concern of malicious participants or people gaining access to records they are not authorized to. Additionally, like all blockchains, a public blockchain would also face scalability issues, and participants running nodes would have to upgrade their hardware as the blockchain got larger and larger.

Many questions remain as to whether or not blockchain will completely disrupt the healthcare industry. Issues with regard to who governs the blockchain and how to prevent it from scaling to enormous size must be figured out before it can released on a large scale. Additionally, companies will have to determine whether or not the current SQL solutions to storing information are sufficient in achieving their goals. Still, the cryptographic nature of the blockchain as well as the ability to share it amongst a set of participants makes it a perfect candidate with regard to interoperability in healthcare. Many blockchain advocates will argue that it is still in its infancy, but the next few years will show if the hype was justified.