Understanding Blockchain: Opportunities in Healthcare

Focus Paper

Neil Pithadia, MS, MBA, FACMPE, FACHE

June 16, 2018

This paper is being submitted in partial fulfillment of the requirements of Fellowship in the American College of Medical Practice Executives.

Introduction

What exactly is the elusive technology behind Bitcoin and does this technology have any application in healthcare? Blockchain, a complex and often misunderstood technology, has caught the public's eye by its speculation and hype built around as a potential universal disruptor.

Let this sink in, if you bought $100 worth of Bitcoin in 2011, its value as of writing this article (April 2018) would be valued near $2,666,666[1]. There's no denying that staggering numbers like that have caught the public and institutional investors' attention. Yet, the underlying technology has several applications to our industry. This focus paper will demystify this technology for the reader, describing how it works and will explore potential opportunities in healthcare through literature search. This paper also will highlight potential applications citing real-world examples such as interoperability, security and smarts contracts in healthcare systems and will summarize the challenges it will need to overcome for adoption. Readers can expect to become aware of Blockchain technology and applications in healthcare after reading this paper.

What is it and how does it work?

Blockchain is a distributed ledger technology that can record transactions between two parties in both a verifiable and efficient manner that becomes a permanent record and yet is open to the public. Historically, we have kept ledgers private; recall your trusty checkbook. The underlying beauty of blockchain is that its applications occur on a public ledger and yet the parties themselves are anonymous. Pioneered by Satoshi Nakamoto, blockchain was originated in the crypts of a mailing list for coders in which he/she developed a whitepaper, "Bitcoin: A

[1] Bitcoin traded at an average of $0.30 per Bitcoin in 2011 and had an average price of $8,000 per bitcoin in April 2018.

Peer-to-Peer Electronic Cash System" (Nakamoto, 2008). "Satoshi Nakamoto" has been determined to be an alias for an unknown individual and/or group. Sounds fishy? Rest assured, the technology itself, if anything, is very human.

Every day, businesses engage in many types of transactions: transaction of tangible, real-world assets or things like contracts or intellectual property. In healthcare, we have a multitude of transactions: claims data, population health information and even personal identifiable information like medical records. All of these transactions require verification, whether it is a prior-authorization or eligibility of provider-payer. The underlying pinning of blockchain is a technology that verifies trustworthiness while making it difficult to manipulate the transaction, itself.

Real-world example

Let's put together an illustrative example to demonstrate how blockchain works. Let's say you have three colleagues that you regularly go out to eat lunch with: Jeff, John and Karen and of course, yourself. Out of camaraderie, your colleagues take turns picking up the tab as it can be inconvenient to exchange cash all the time. Say you keep a joint ledger online on a website for transactions and then settle up at the end of the quarter.

An example of one quarter's ledger may be:

Joint Ledger Q1, 2018
-Jeff pays $30; attendees: Jeff, John and You
-John pays $40; attendees: All
-Karen pays $10; attendees: Jeff and Karen
-You pay $30; attendees: Jeff, Karen and You

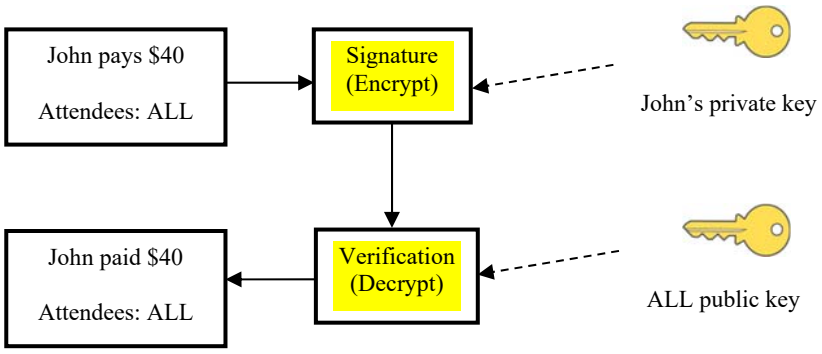
As mentioned this ledger is online and open to the public (in this example, the public consists of our three colleagues and yourself). These individuals can add transaction lines as they input their entries and at the end of the quarter everyone gathers to settle up.

So an example of the transaction of John paying $40 with all attending will look like the following:

	Debit	Credit
John		
Meals Expense	$10	
Accounts Receivable	$30	
Cash		$40
John (when receives monies at the end of the quarter)		
Cash	$10	
Accounts Receivable		$10

	Debit	Credit
Jeff/Karen/You		
Expense	$10	
Accounts Payable		$10
Jeff (when pays John)		
Accounts Payable	$10	
Cash		$10

You might be thinking, "wow, we must have some very trusting colleagues to enter their own transactions!" The issue is how we prevent illegitimate transactions from being recorded. For example, if John places a transaction of "John pays $100," how is the transaction verified? In the non-digital world, we would likely request the receipt and have all attendees sign off and verify that the transaction was indeed correct. Blockchain solves this issue by verification through a digital signature called a Private/Public key pair. As the names appear, the private key is essentially a signature that only the individual four people have to themselves, whereas the public key is an identifier of the person given each transaction. The private key prevents forgeries from occurring. So say the transaction is "John pays $40," John would place this transaction and then sign with his private key, and then Jeff, Karen and You would have to verify that transaction with your public keys. Below is what this would look like:



These keys are formed under what computer coders called a cryptographic hash function. A hash function is an algorithm that takes an input of any size and turns it into an output with a fixed size.

Say, for example; you have a string of numbers as your input:
2 4 6 8 10 12 14

The hash function says to sum all the numbers up:
2+4+6+8+10+12+14

In this case, the output would be 56; quite simple. A computer could quickly guess the string of numbers and validate the correct input. The beauty of cryptographic hash functions is that it is very easy to take inputs to derive an output, but extremely difficult to take an output and determine the inputs. Said simply, there are several ways to derive a string of seven numbers to add up to 56.

It's secure. The cryptographic hash function for Bitcoin is called Secure Hash Algorithm 256-bit or SHA-256. Without going into the technical details of this, essentially this means it is extremely secure. In order to guess the right private key for that transaction, the probability would be 2 to the power of 256.

It enables rules. You may be thinking how does the system prevent excess spending? For example, what if Karen racks up $20 in debt and doesn't settle? Well, first off, it's time that the group finds a new colleague to go to lunch with, but perhaps the more creative answer solved by

the architects of blockchain, is that you never have to settle if everyone pays something in the beginning and the system does not let them spend any more. So say our four colleagues each put $50 per quarter. The transactions would look like the below:

Ledger:

1.) Jeff gets $50
2.) John gets $50
3.) Karen gets $50
4.) You get $50

Karen's Balance

3.) Karen gets $50 → $50

The next few transactions may be:

5.) Karen pays Jeff $20 → $30
6.) Karen pays John $30 → $0

7.) Karen pays You $20 (INVALID) → OVERDRAWN

The system must recognize that Transaction 7 is an invalid transaction as Karen has overdrawn and cannot send you $20. Therefore, the system must be able to verify all transactions up to that point. Interestingly enough, this history of transactions is literally the currency of Bitcoin.

It's decentralized and scalable. In our example, it is mentioned that this ledger is on a website where the four individuals could add new transactions. This system is still centralized in that the central authority is the four individuals that keep track of each other's money, much like a bank. Blockchain works on a decentralized system. That is, everyone has their own copy of the ledger. A decentralized data registry of transactions, blockchain, has the ability to transform industries. HBS Professor, Lakhani, describes the future of blockchain as the following in his paper, "The truth about Blockchain."

> With Blockchain, we can image a world in which contracts are embedded in digital code and stored in transparent, shared databases where they are protected from deletion, tampering and revision. In this world every agreement, every process, every task and every payment would have a digital record and signature that could be identified, validated, stored and shared. Intermediaries like lawyers, brokers and bankers might no

> longer be necessary…this is the immense potential of blockchain. (Iansiti & Lakhani, 2017)

This technology can be applied to exchange of goods and services, supply chain, and contracts in healthcare and there are some big names making considerable investments in this technology in the healthcare space.

III.) Blockchain opportunities in healthcare

Interoperability

Whether to scale, corner the market or add new lines of business, mergers and acquisitions (M&A) have become commonplace in our industry. 2017 was no exception as it was one of the busiest years in M&A activity in the last two decades (See Figure 1). The core challenge with scaling is the information system(s) that supports different health systems. These information systems must be agile enough to allow health systems to scale into newer or alternative services. For health systems, it will then be imperative for these systems to talk; interoperability with legacy systems. It should then be no surprise that an overwhelming majority of senior IT healthcare executives indicated focusing 2017 on improving interoperability in a survey for which type of Electronic Health Record (EHR) development projects they would focus on (Siwicki, 2017).

Why is it that interoperability has been so elusive? For quite some time now, health systems have been awaiting EHRs to communicate. While incentives have been made to make healthcare data more accessible, very little has been done to allow them to communicate, at least not safely. As a result, clinical teams are spending more time with data entry rather than direct interaction with patients. In a time where patient experience and clinician burnout is becoming increasingly important, there is a large opportunity for breakthrough technology. The

Association of American Medical Colleges (AAMC) reported that 54.4% of physicians reported at least 1 symptom of burnout 2014 up from 45.5% in 2011 (AAMC).

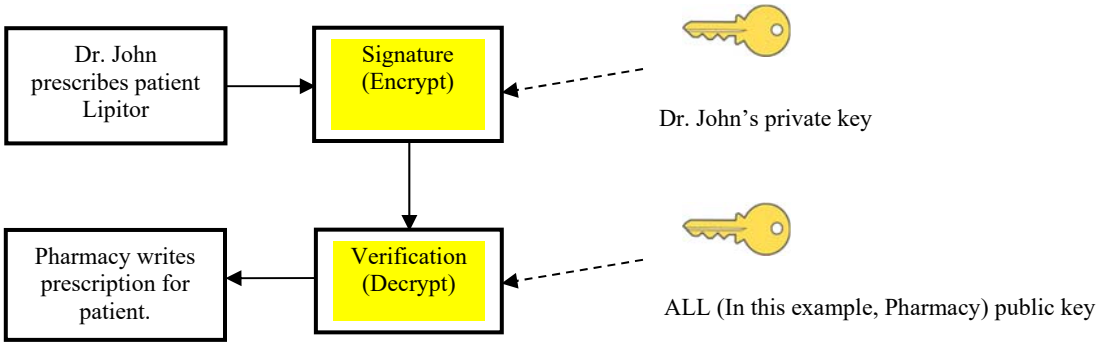
There are three models of interoperability among medical data; push, pull and view as per visionary Dr. John Halamka, Chief Information Officer at Boston-based Beth Israel Deaconess Medical Center.

> **Push** is the idea that a payload of medical information is sent from one provider to another. In the U.S. a secure email standard called Direct is used to provide encrypted transmission between sender (for example, an Emergency Room physician) and receiver (for example, your primary care doctor)…**Push is a transmission between two parties, and no other party has access to the transaction.** If you end up being transferred to another hospital, the new hospital may not be able to access data about your care that was pushed to the first hospital.
>
> **Pull** is the idea that one provider can query information from another provider. For example, your cardiologist could query information from your primary care doctor. As with push, all consent and permissioning is informal, ad hoc, and done without a standardized audit trail.
>
> **View** is the idea that one provider can view the data inside another provider's record. For example, a surgeon in the hospital operating room could view an X-ray you had taken at an urgent care center. Security approaches are ad hoc, not audited in a standardized way, and not necessarily based on an existing patient-provider relationship. (Halamka, 2017).

The fourth model is **blockchain**. Consider this, a central EHR in which any update to a patient's history is immediately updated on a community-wide ledger centered around the patient's history. There would involve no manual human intervention to update or reconcile this data at any point of service (Pharmacy, Acute Care, Physician, Telehealth, etc.), and one could have access to the full history of an individual. One would imagine this is what the architects of preliminary EHRs envisioned decades ago.

Let's go back to our colleague's lunch ledger to see how this might look under a blockchain-powered EHR transaction. In this example, our patient lives in Northern California.

A road-warrior, he travels as a partner at an accounting firm. During an annual wellness visit, our patient is noted to have high cholesterol and his Primary Care Physician (PCP), Dr. John, prescribes Lipitor to address this. This transaction is seen below, where the public key is held by "ALL" trusted healthcare providers (Pharmacy, Acute Care, Physician, Telehealth, etc.) that are permitted to have access to this information. There are many modes of who controls this access; it could be a singular group such as the government or perhaps a less totalitarian approach, control is granted by the patient as the custodian of their transactions. In this example, the public key to accessing the prescription for our patient by Dr. John is verified by the pharmacy.



Now, what happens if our patient is in Texas for business and falls ill and in need of an antibiotic? Under our current environment, he could contact Dr. John and perhaps through a tele-platform, Dr. John, who is currently taking care of the patient, could add the order for a prescription into their own system and send it to a local pharmacy in Texas either electronically or perhaps by fax. If our patient goes to a local physician in Texas and likely said physician is independent of Dr. John in California, the local physician would have to add Lipitor (along with any other medications our patient takes) and the antibiotic. Now imagine how many transactions like this take place daily and how much error is involved in the process. Many studies have described medication errors, but data is difficult to measure across the care continuum. In a UK study, 5% of PCPs prescribed/monitored errors in prescriptions, a Swedish study found a 42%

medical error rate and a study in Mexico found medication errors as high as 58%. The unifying theme is that this is a global issue (WHO, 2016). This is the potential beauty of blockchain. With blockchain, each prescription would be an entry into the system, much like our colleague's lunch example. Whenever a prescription is discontinued, the chain will withdraw the transaction, and therefore, the most recent blockchain would contain the balance of the current active drugs for the patient. Here's the kicker, any health provider would be able to view this information if they had a public key that is permitted to the transaction.

Perhaps you're a pessimist and think this is too far-fetched. Dr. Halamka has taken this from concept to a working product at MIT MediaLab, called MedRec. In the last year, they have been piloting blood work, vaccinations, prescriptions and treatments at Beth Israel Deaconess Medical Center, a world-class teaching hospital at Harvard Medical School.

> Every time a digital transaction takes place, bits of code group it into an encrypted block with other transactions happening at the same time. For bitcoin, this would be a flurry of buying and selling. For EHRs, it might be all the things that happen to you on a doctor's visit (blood work, a new prescription, maybe some X-rays). Then people validate the transactions—in health care, likely a physician or pharmacist trusted with an access [public] key. Then the software timestamps each validated block and adds it to a chain of older blocks, in chronological order. The sequence shows every transaction made in the history of that ledger, whether it be bitcoin sales or a knee replacement procedure. (Molteni, 2017).

MedRec is impressive in its own right. However, skeptics may point at its narrowness only impacting a segment of a Boston hospital system. What about a blockchain health system for an entire country? The recent collaboration between Guardtime and Estonian eHealth Foundation demonstrates that blockchain technology can potentially be scaled to an entire country. The two formed a proprietary Keyless Signature Infrastructure (KSI) to secure the health records of its one million citizens of Estonia as a response to a 2007 cyberattack (Wikipedia). KSI allows the Estonian citizens to verify the integrity of their records on governmental databases. Each citizen

has an online e-health record that is identified by an electronic ID-card (private key). Their EHR is a centralized national database and permits users like various healthcare providers, public keys to the database. (E-estonia, 2018). While there is still considerable work needed, KSI is currently in its proof of concept phase for over a million users.

Security

A key advantage of blockchain is its security. According to Protenus Breach Barometer report, there were a total of 477 health data breaches in 2017, up 27 from the previous year, affecting 5.6M patient records (Protenus). As cybersecurity continues to become a significant threat, healthcare is caught in the cross-hairs of this threat. This is where blockchain is extremely disruptive. Due to the inherent nature of the blockchain and the SHA-256 function we described earlier, the probability of hacking through computational guesswork is 2 to the power of 256. It is incredibly difficult from a computing power standpoint to guess the correct key to gain access to the transaction. Even by brute computing force it is very difficult for an individual or even a conglomerate to achieve this.

A blockchain-based EHR could unlock the true value of interoperability and security. This system has the potential to eliminate the high costs associated with third-party vendors. The true value of such a technology is its ability to decrease unnecessary service, duplicate tests and ultimately lowering costs across the care continuum. That said, a more near-term opportunity for this technology is through Smart Contracts.

Smart Contracts

Smart contracts enable individuals and parties to exchange assets or currency while avoiding services of a middleman, typically an attorney or notary. The beauty of smart contracts in the context of blockchain is that the rules and penalties around a traditional agreement are

automatically enforced. Go back to our colleague's shared ledger example, Karen is unable to pay you $20 as she is overdrawn. The system will recognize this rule and the transaction will be unable to go through as it is automatically enforced in the rules that are constructed. In healthcare, smart contracts can range from asset tracking to transaction/claims management, as described below.

Asset Tracking

The drug industry has a sizable counterfeit issue. The EU Intellectual Property Office (EUIPO) estimates that the pharmaceutical industry loses €10 billion annually directly as a result of the presence of counterfeit medicines in the EU marketplace, working out at 4.4% of total sales (Pharmafile). The management of asset tracking through a technology such as a blockchain can have sizable benefits. A blockchain-based technology could ensure a custody log to track each supply of the supply chain. This can be verified through private keys within the chain to develop proof of ownership of the drug across the supply chain. At current, there is no actual technology in use. There are notable research projects that are still at the advanced planning stages. IBM is tackling the issue of counterfeit drugs in Kenya and East Africa. The port of Mombasa is an entry point of counterfeit drugs sourced from China and India. The most common drugs include antimalarial. A staggering 122,000 children under the age of five in Africa die due to counterfeit antimalarial drugs (NPR). The counterfeit market have become masters at making their products look authentic; from size to packaging, they appear to be identical even including official regulation seals/holographic stickers.

IBM research is targeting a solution involving a permissioned blockchain and a mobile interface. Each party attached to the supply chain of the drug is certified and authorized to complete, track and verify transactions on a blockchain. This includes the drug manufacturers,

carriers, hospitals and clinics that dispense the drug. Verification is critical and accomplished through a mobile interface and Quick Response (QR) code scans associated with the serial numbers of the drugs. Therefore, any person ordering drugs on the blockchain-based network is assured of getting industry-approved products (Bitcoin Africa).

IBM's endeavor is not alone. Management consultant, Accenture's Primrose Mbanefo, formed a working group called Hyperledger Project to target this space (Wiki Hyperledger) and a company called iSolve LLC is working with multiple biopharma companies to implement an Advanced Digital Ledger Technology (ADLT) termed BlockRx to manage the drug supply.

Transaction/Claims Management

Another large opportunity is Claims and Billing management. In the United States, The National Health Care Anti-Fraud Association estimates, conservatively, that health care fraud costs the nation about $68 billion annually — about 3 percent of the nation's $2.26 trillion in health care spending (May).

Blockchain-based systems can provide solutions for minimizing these medical billing-related fraud costs. By automating the claim adjudication and payment processing, blockchain-based systems could reduce the administrative costs and time for providers and payers. Recently, Gem Health, a provider of blockchain application platforms for enterprises, has collaborated with Capital One to develop blockchain-based healthcare claims management solutions (Bitcoin Magazine). A major pain point in our industry is the amount of time it takes for claim settlement. In our ecosystem, currently, it can take an electronic claim anywhere from 7-14 days to process payment and upwards of 9 weeks for paper claims, from plan to plan. This is the golden opportunity for smart contract applications employing blockchain technology. The smart

contracts could contain the payer-provider terms and submission could generate real-time payment.

Conclusion

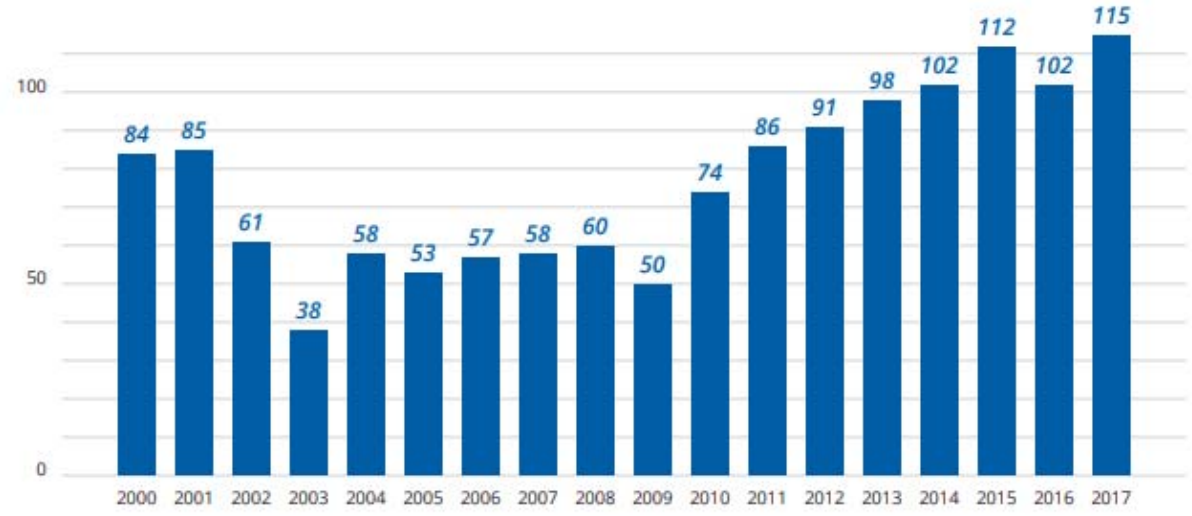
Healthcare is tough. Change is extremely difficult in our industry. Yet, our industry is embracing technologies like blockchain. While there is significant disruption power behind blockchain, it is a technology in its infancy. Furthermore, the hype of blockchain as a transformative technology will need to overcome regulatory constraints and significant challenges that keep the status quo.

The challenge to have blockchain adoption to applications like interoperability in healthcare will be the development and governance of the underlying platform. To get there will involve significant technological and conflicting interests' changes. In the case of interoperability, data extracted from independent EHRs would have to be cryptographically recorded to an open platform and shared ledger. There will be significant conflicting interests as independent EHR vendors would inevitably maintain their closed systems as they seek to protect their market share and profits. This is a formidable challenge that will take time. However, perhaps government intervention is the answer. Even before the government can support this effort, we must agree upon a set of standards and contracts along with a body of governance that would oversee it. The Estonia KSI project will be particularly interesting to observe over the next few years in the adoption of a blockchain technology at a national scale. Even then, a controlled environment of a million citizens vs. most first-world countries is leaps and bounds apart. Even near-term applications such as smart contracts including asset tracking and claims management are at conceptual and early-developmental stages. In a 2017 survey by IBM amongst 200 healthcare executives, 16% expected to have a commercial blockchain solution at scale in the

next year. Paradoxically, the survey also showed that healthcare executives don't anticipate much disruption ahead by blockchain due to regulatory constraints and framework challenges of the healthcare industry (IBM).

Appendix

Figure 1- Hospital and Health System M&A Activity, 2000-2017



Source: Kaufman Hall Transactions Data

References:

AAMC. Exploring Resilience: What do we know? https://www.aamc.org/download/468430/data/physician-resident-and-medical-student-burnout.pdf

Bitcoin Africa. How the Blockchain Can Prevent Drug Counterfeiting in Kenya. http://bitcoinafrica.io/2018/01/18/blockchain-prevent-drug-counterfeiting-kenya/

Bitcoin Magazine. Gem Partners with Capital One for Blockchain-based Health Care Claims Management. https://bitcoinmagazine.com/articles/gem-partners-with-capital-one-for-blockchain-based-health-care-claims-management-1477502028/

BlockRx. https://www.blockrx.com/isolve-and-the-blockrx-project-7-pharma-use-cases-for-the-blockchain-for-2017/

E-Estonia. (2018). E-health records. https://e-estonia.com/solutions/healthcare/

Halamka, John MD, Lippman, Andrew and Ekblaw, Ariel. (2017). The Potential for Blockchain to Transform Electronic Health Records. *Harvard Business Review.*

Iansiti, Marco & Lakhani, Karim. (2017). The truth about Blockchain. *Harvard Business Review.*

IBM Institute for Business Value. (2017). Healthcare rallies for blockchains, keeping patients at the center. https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03790usen/GBE03790USEN.PDF

KaufmanHall. (2017). 2017 In Review. The Year M&A Shook the Healthcare Landscape. https://www.kaufmanhall.com/sites/default/files/2017-in-Review_The-Year-that-Shook-Healthcare.pdf

May, David. (2010). The New Fraud Offensive. *Modern Healthcare*. http://www.modernhealthcare.com/article/20100628/MAGAZINE/306289998

Molteni, Megan. (2017). Moving Patient Data is Messy, but Blockchain is here to help. *Wired.* https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/

Nakamoto, Satoshi. (2008). Bitcoin: A Peer-to Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

NPR. (2015). Fake Medicines Do Real Damage: Thousands Die, Superbugs Get Stronger. https://www.npr.org/sections/goatsandsoda/2015/04/24/401948030/fake-medicines-do-real-damage-thousands-die-superbugs-get-stronger

Pharmafile. Five Worrying Facts about Fake Medicine. http://www.pharmafile.com/news/513663/five-worrying-facts-about-fake-medicine

Protenus Breach Barometer Report: Year in Review. https://cdn2.hubspot.net/hubfs/2331613/Breach_Barometer/2017/Annual%20Report/2017%20Breach%20Barometer%20Annual%20Report.pdf

Siwicki, Bill. (2017). The Year Ahead in Healthcare Information Technology. *Healthcare IT News.* http://www.healthcareitnews.com/news/2017-year-ahead-healthcare-information-technology

World Health Organization. (2016). Medication Errors. http://apps.who.int/iris/bitstream/handle/10665/252274/9789241511643-eng.pdf

Wiki Hyperledger. https://wiki.hyperledger.org/requirements/use-cases/use-case-counterfeit-drug-prevention-and-detection#business_problemopportunity

Wikipedia. 2017 Cyberattacks on Estonia. https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia