Blockchain: Next-Generation Healthcare

Exploratory Paper

Susan Krpata-Young, FACMPE

August 31, 2018

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

Introduction

The government's big push toward electronic health information exchange (HIE) began in 2009 with President Barack Obama's signing of the American Recovery and Reinvestment Act (ARRA), but despite government initiatives and massive effort and investment put into health information systems and technology, the full promised benefit of electronic health records (EHRs) is yet to be realized. One reason for its failing could be because EHRs were not designed to manage multi-institutional, lifetime medical records, so as life events take patients away from one provider's data silo and into another they leave data fragmented across various organizations. In doing so, they lose easy access to past data, as the provider -not the patient- generally retains primary stewardship through default arrangements in the process of providing care. Subsequently, the significant increase in the use of electronic health records and other health care related technology has created a wealth of electronic information that is increasingly being targeted by cyber attackers since patient health information (PHI) has tremendous value on the black market. The adoption of digital patient records, increased regulation, provider consolidation, and the increasing need for information exchange between patients, providers and payers, all point towards the need for better information security and control over the data.

The lack of more effective security and control over this wealth of electronic information has unfortunately opened the door for the healthcare industry to be one of the most targeted by cybercriminals due to its heavy reliance on technology and vast amount of valuable patient data. Patient safety is not just about physical and emotional well-being and protection; it also includes the safeguarding of patient electronic health records and intellectual property rights.

The healthcare industry was a lucrative target for hackers in 2017 as weaponized ransomware, misconfigured cloud storage buckets, and phishing emails dominated the year. In 2018, these threats have continued as cybercriminals get more creative despite better awareness among healthcare organizations at the executive level for the funding needed to protect themselves:

> The U.S. Department of Health and Human Services estimates that significant breaches of medical data and patient records happen once every 1.75 days. Think about that – over two hundred breaches of medical records in the U.S. alone, and those are only the ones actively known and disclosed. The costs of these breaches are enormous, for patients and providers. Patient data suffer violations of their privacy, including identity theft, and threats of blackmail, while providers must handle loss of trust, reputational damage, and fines of up to $50,000.00 per stolen record. Smaller clinics are especially vulnerable to damage from breaches and hackers. Clearly, with the current state of healthcare something isn't working.[1]

The consumerization of information technology (IT) and the bring-your-own-device (BYOD) movement in the workplace enables providers to access patient data, billing information, clinical trial data, and employee information on the go. However, convenience comes with a price; data now resides on desktops, laptops, smartphones, tablets and USB drives. Given the rise of mobile computing and BYOD in healthcare, the once straightforward process of protecting private health data has evolved into a more complex and nuanced undertaking. According to a study published by Crowd Research Partners, one in five companies suffered a data breach involving mobile devices.[2]

For a healthcare organization subject to large-scale information technology (IT) incident, a data breach can represent hundreds of millions in cost for identity theft protection, IT forensics, and government fines. Given the significant value of healthcare data, such as social security numbers, treatment records, financial data, and more sensitive personal information, the cost of a breach to a hospital or health system can be destructive. One must wonder why the health industry, as it relates to the management of electronic health records (EHR), lags behind other industries in data security. Yet, healthcare is one of the most critical aspects of our socio-economic infrastructure.

Numerous electronic health records system applications are available on the market to service every specialty and hospital imaginable, yet the sharing of secured patient data, in a universal way, remains problematic and disparate. The issue within the healthcare industry, as it relates to data security, remains how to store and enable permission to share critical data with more stakeholders, all while guaranteeing data integrity and protecting patient privacy, safety, and financial information. Perhaps the reason why the healthcare industry lags behind others is because of the massive scale of the landscape, and the fact that industry outsiders most likely lack sufficient insight to gauge the priority of healthcare issues. With such a huge endeavor, health information technology (HIT) professionals are turning their focus towards proven technologies and looking for healthcare problems to solve with it, and this may very well be the case with the emerging disruptive technology known as *blockchain*.

To provide research for this paper, an extensive literature review was conducted focusing on blockchain and blockchain in healthcare to include e-books, white papers, scholarly articles, e-publications, online journals and newsletters.

Purpose

The healthcare industry is on the verge of disruption in its digital infrastructure, as the current system does not fully support the security or interoperability that is inherently necessary. This paper aims to illustrate possible influences, goals, and potentials connected to disruptive technology. It will serve as exploratory research to substantiate why blockchain technology is thought to be the next-generation solution in healthcare, and why so many health information technologists (HIT) endorse the migration towards encrypted hyperledger and horizontal architecture as a means to secure and protect patient data from breaches, and improve overall efficiencies across all medical ecosystems.

Background

ARRA was designed to (among other things) improve the nation's healthcare delivery system by digitizing all patient records. In March 2010, President Obama signed comprehensive

healthcare reform, the Patient Protection and Affordable Care Act (ACA), into law. The law aims to make health coverage more accessible and affordable for many Americans, while improving quality and reducing costs. It is important to remember that the biggest impact on electronic health record (EHR) usage was contained in the 2009 ARRA law, which includes the "Health Information Technology for Economic and Clinical Health (HITECH) Act". The HITECH Act supports the concept of electronic health records – meaningful use [EHR-MU], an effort led by Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health IT (ONC). HITECH proposes the meaningful use of interoperable electronic health records throughout the United States healthcare delivery system as a critical national goal. Meaningful use, in a health information technology (HIT) context, defines minimum U.S. government standards for using electronic health records (EHR), and for exchanging patient clinical data between healthcare providers, between healthcare providers and insurers, and between healthcare providers and patients. In using certified EHR technology the provider must submit to the Secretary of Health & Human Services (HHS) information on quality of care and other measures. Given the kinds of structural changes embedded in the ACA and the changes happening in healthcare in general, health information technology (HIT), including EHRs, are a necessary platform for facilitating such changes.

Healthcare is one of the few mega industries whose data management systems are designed by people who do not use them on a daily basis. Doctors, healthcare providers, allied workers, administrative personnel, and patients depend upon these programs for efficiency and control, yet they have had little input with the development of such programs and data methodologies. Even with all the disparate and numerous digital practice management software applications available for healthcare providers today, they often fall back on providing a piece of paper for the patient to carry to the pharmacy or a report or testing result to their next appointment. Far too many healthcare systems are dependent on spreadsheet-based tracking,

manual processes, and disconnected reporting structures. The same disconnect applies to supporting procurement and supply chain systems covering the course-to-pay process.

Patient data and the sharing of the data is living in a deconstructed data ecosystem, while the people who control the data do their best to follow mandates requiring them to adhere to ever increasing privacy, security, and compliance guidelines. These same people are expected to accomplish all of this work while at the same time shifting gears away from fee-for-service to fee-for-value models, e.g. Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Occupational Safety and Health Administration (OSHA), and Centers for Medicare & Medicaid Services (CMS) value based programs: Physician Quality Reporting System (PQRS), The Medicare Access and CHIP Reauthorization Act of 2015 (MACRA): Merit-based Incentive Payment System (MIPs) and Alternative Payment Models (APMs), Advancing Care Information (ACI) and Quality Payment Program (QPP).

In order to meet the ACA requirements that 80-85% of all premiums are spent on healthcare services and activities, providers must mature their spend management capabilities, from tracking to reporting. Risk, supplier and contract management tools help providers ensure compliance and avoid paying associates rebates and penalties, as required by the Physician Payment Sunshine Act of 2014 (PPSA).

As both federal and state regulations continue to compound, providers find it difficult to maintain efficiency and control of the data. However, without end-to-end data governance and spend management solutions, healthcare providers do not stand a chance of keeping up with the regulatory requirements of HIPAA, the Physician Payment Sunshine Act (PPSA), and similar ACA standards. As enforcement shifts unpredictably in practice and focus, healthcare providers are compelled to prepare by developing best practices in risk management and data governance. Only by streamlining business processes throughout their supply chain can providers expect to maintain compliance, stay competitive, and provide high quality services:

> Healthcare is big business, but the money doesn't come easy. To maximize profits while optimizing patient care, healthcare providers are increasingly turning to digital technology solutions. In 2017 margin-eroding pressures squeezed providers on all sides. In 2018, it is more critical than ever to create and sustain significant efficiency improvements and enable deeper supply chain collaboration through strategic deployment of enterprise-wise management platforms. Given the constant evolution in regulations and business models, technological agility is a critical requirement.[3]

The electronic information systems used today within the healthcare world, not being designed by regulators, health professionals, accountants, etc., are inefficient, complex, and most importantly, very costly. What is needed to shift away from this marginalized healthcare system towards a better healthcare system is horizontal integration to enable the whole ecosystem to have better interoperability across all channels. Now that corporate technology and finance giants like Amazon, JP Morgan, and Berkshire Hathaway are entering the healthcare market, the pressure to digitally transform is even more intense.

Patient expectations are moving towards a more coordination continuum of care, and they increasingly prefer one-stop-shopping. Consolidating services, prioritizing programs, and leveraging increased purchasing power into more competitive contracts will require tools that can punch through data and reporting silos. Deploying a unified streamlined source-to-pay process will minimize the role of disparate managers and clinicians in transactional procurement activities and maximize compliance and auditability. This horizontal integration can be realized with blockchain, whereby a distributed data centric ledger becomes the backbone for efficiencies, controls, and compliance.

Body

To date, medical data within each medical ecosystem has had three data models; Pull, Push and View. Computer scientists and health information technologists (HIT) worldwide are challenged to develop alternatives to the Pull vs Push technology.

Pull Technology vs Push Technology		
	Pull Technology	**Push Technology**
Definition	A client that requests information from a server.	A server that initiates information updates to a client.
Example	A web browser requests a web page.	An email server transmits an email to an email client.

- **Pull** technology refers to clients that make requests to servers. This is the traditional way to structure client/server architecture.
- **Push** technology refers to servers that initiate information updates to clients.
- **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 previously taken at an urgent care center.

The difference between Pull vs Push technology comes down to who initiates information updates. If the client initiates requests, it is Pull. If the server initiates updates, it is Push. Each slice has advantages and disadvantages, with each suffering from data silos and a lack of interoperability among domains, resulting in an enormous number of disconnected databases. The obvious problem with *information silos* and their insular nature, incapable of reciprocal operation with other that are or should be related, is that patient data is touched by many disparate medical professionals in different data ecosystems, each having their own central data rules and influences. This problem affects not only healthcare providers needing access to the PHI to provide the best patient care, but also the patient, who might have to complete extra forms to release medical records or wait for a busy office to transfer lab results.

Because of many points of data entry and permissibility, the quality and security of patient medical data are often compromised in multitudes of ways. As a means to address the problem, disruptive innovation is driving the future of health and healthcare. Open source software technology is considered to be the answer to securing critical lifetime medical record sharing across all supporting platforms and is expected to revolutionize the way electronic health information is managed by decentralizing data collection, and profoundly increasing data security and transparency. This disruptive breakthrough, open source software called blockchain, is one of the most innovative technologies to be realized since the deployment of the Internet and world-wide-web.

Beyond the Pull, Push and View interoperability models, blockchain is a different construct, providing a universal set of tools for cryptographic assurance of data integrity, standardized auditing, and formalized *contracts* for data access. Blockchain is touted to be the next-generation IT technology to provide a compelling solution to reduce errors, enhance system intraoperatively, and improve data quality. It is capable of creating a primarily security driven ecosystem that will enable providers to access private health records (PHR) faster, coordinate patient care more efficiently, and communicate with their patients, seamlessly and securely:

> The so-called distributed ledger technology was developed in 2008 by Satoshi Nakamoto, a possibly pseudonymous person (or perhaps multiple people) who designed it as the underpinning for the exchange of the digital cryptocurrency known as Bitcoin. Health information technology and information security specialists are hearing a lot about blockchain these days. "It's the answer to interoperability. And the technology can solve healthcare's looming security problems, as noted by Healthcare IT News editor, Mike Miliard,[4]

What is blockchain and how does it work

You cannot discuss the history of blockchain technology without first starting with a discussion about Bitcoin. Shortly after Nakamoto's whitepaper was released, Bitcoin was offered

up to the open source community in 2009. Blockchain provided the answer to digital trust because it records important information in a public space and does not allow anyone to remove it. Ordinary digital recordkeeping systems rely on a central administrator that acts as gatekeeper to a treasury of data. Blockchain, by contrast, employs a network of synchronized, replicated databases. It is a stream of data (a distributed ledger) that is written, shared with and confirmed by a collection of nodes on a common network, run by different companies or organizations. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Information is scattered among these nodes, rather than on a single server, and is exchanged through encrypted, peer-to-peer pathways. Each transaction is visible to every computer on the network and must be approved by a majority in order to be successfully completed. Each batch of transactions, or block is date-and time-stamped, marked with the user's identity, and given a cryptographic code, which is posted to every node. These blocks form a chain, preserved in an electronic ledger that can be read by all users but cannot be edited. Any unauthorized access, or attempt at tampering, can be quickly neutralized by these overlapping safeguards. Even if a hacker managed to break into the system, penetrating deeply would be extraordinarily difficult.[5]

Blockchain was designed to deal with transactions involving value: information, data, money, property, bill payments, money transfer, work, votes or other goods, and is often compared to a ledger. As in a traditional paper-based ledger, one can only append data and can never delete or manipulate existing data. The crucial distinction between the two is that the blockchain is present in many identical copies on many different computers.

Rather than a central database, the blockchain record can be distributed and shared across networks, with credentialed users able to add to, but not delete or alter, the transaction log. The validation step is the key that allows a blockchain to replace a trusted intermediary. The validation and immediate confirmation from the whole of the network, and the distributed at-all-times nature of the chain, builds trust in the system as a whole. An example of this would be if

any node on the network tries to transfer a particular asset twice, to two different parties, that transaction would not be validated by others on the network, and there would be no agreement to add it as a new block on the chain. The same rules apply to everyone, and we do not need to depend upon just one party to set those rules and keep the ledger consistent and honest. Transactions are encrypted and require permissions by the network to be accessed.

When entrepreneurs understood the power of blockchain, there was a surge of investment and discovery to see how it could impact supply chains, banking, healthcare, insurance, transportation, voting, contract management and more. For example, the big banks see blockchain as an opportunity to improve process services by making them cheaper, faster, and more efficient by using the technology that underlies cryptocurrency Bitcoin. In fact, banking and financial markets are adopting the technology dramatically faster than initially expected. "Nearly 15% of financial institutions are currently using blockchain technology."[6]

Potential benefits of blockchain technology in healthcare

The following demonstrates most of the potential benefits of adopting distributed ledger technology in the healthcare industry, and how it can resolve healthcare's looming security problems across networks:

Better Security and Backups – Blockchain can be applied to protect internal infrastructure within an organization. Having many copies on the blockchain ledger within a healthcare organization with independent parties having access to the separate copies under lock and key creates redundancy like we have never seen before. If implemented correctly, blockchain would protect against ransom attacks and other types of catastrophes like data corruption or hardware failure.

Effective and cost efficient - Streamlined and hassle-free data sharing across key healthcare providers plays a pivotal role by offering benefits like cost- efficient-treatments, precise diagnosis, and eventually better cures for various diseases. By utilizing the blockchain

technology, the healthcare providers can work simultaneously with the help of networks with enabled shared access. Effective data tracking and powerful security provisions are other purpose-specific features offered by blockchain technology. Uniformity, agility, quality, and security are other key benefits.

Powerful monitoring - One of the key issues for ensuring a better healthcare management network is constant, powerful monitoring. As a precise response, the blockchain technology allows for documenting the transactions in a decentralized record. It enhances precision and brings transparency while at the same time saving crucial resources like time, cost and effort.

Better collaboration - To a great extent, the success of any public healthcare initiative depends upon the collaboration of various parties involved and deep insights into vital healthcare trends. With the help of distributed ledger technology, the blockchain proactively promotes the innovation in the field by empowering key participants to collaborate and group research.

Healthcare sector convergence - The transition to fee-for-value models is intended to drive down healthcare costs on a national scale, but new models and structures will be beneficial to providers if they are able to visibly enhance spending and executive strategic sourcing initiatives. Healthcare systems can reduce their operational burden by streamlining procurement processes and deploying intelligent automated solutions across the enterprise.

Transparent and organized processes – Since healthcare is a crucial industry, it is very important to ensure a well-organized methodology, as well as transparent processes. At the same time, high-end security and 100% accuracy are equally, if not more, important. Blockchain technology not only results in integrated healthcare information, but also maintains traceable records of distributed data and work. The public/private key access strongly safeguards the overall security by eliminating chances of data leakage. Blockchain technology also facilitates tracking the movement of a drug from producer to the patient. Apart from ensuring timely supply, it eliminates the chances of counterfeiting.

Easy access and budget control - The uninterrupted connectivity with level-based authorization and easy access greatly empowers providers and researchers. By automating the tedious processes, the blockchain technology helps the healthcare industry to extract the maximum potential of manpower during different phases and processes. As a result, it enhances the human productivity, and increased productivity means better output in a shorter span of time. By enabling dividing the processes into different phases, the blockchain technology also helps to keep the budget under control, lowers administration costs and allows a better, purpose-specific utilization of allocated funds.

Bringing Down Healthcare GDP – Blockchain can be leveraged to bring down spending on the U.S. gross domestic product (GDP) for fraud and duplicate charges for procedures and discrepancies using the technology for medical billing. CMS estimated that health care spending will account for 19.9 percent of GDP by 2025, up from 17.8 percent in 2015.[7]

Protection of crucial data - Equipped with the latest cryptographic features, the blockchain technology not only facilitates checking the data authenticity with the help of digital signature but also it helps in offering foolproof security of the data; thus it offers a precise solution to the twin issues of trust and security.

Extracting the best benefits - While there are diverse points of digitally collecting the healthcare data, it is even more important to extract the best benefits out of this healthcare data without complicating the processes. For that purpose, the portability and uniform compatibility of the data while working across diverse systems are very important. Due to its keen focus on streamlined flow, uniform portability, and multi-faceted protection systems across different phases, the blockchain technology perfectly handles diverse present challenges as mentioned above. Collectively, it helps in extracting the maximum output from the data collected on diverse levels.

Distributed ledger technology - Information held on a blockchain exists as a shared and continually reconciled database. By allowing digital information to be distributed but not copied,

blockchain technology created the backbone of a new, more commercially viable, Internet, e.g. Public blockchain technology is a proven secure P2P (peer-to-peer) ledger system that uses public key encryption to protect information, (e.g. Bitcoin).

Potential challenges of blockchain technology in healthcare

As with any innovation that can disrupt old methodologies to provide new solutions and benefits, there will always be potential challenges and new problems to address and solve. The following demonstrates some of the potential pitfalls of adopting distributed ledger technology in the healthcare industry:

Resistance to change - Proofs of concept have been developed which bring blockchain technologies into the healthcare industry; however, there are still many barriers to adoption. One of the most significant barriers will be the inherent resistance of the healthcare industry to change its current practices, especially relating to organizational, structural, technological, and human factors. With so many well entrenched business models and existing data management adaptations currently in use, it may be years before the healthcare industry is capable of fully utilizing distributed ledger technology as an application across all medical ecosystems.

Research and Development – R&D will prove costly, and it will require the cooperation of government, private enterprise, vendors and other entities to all agree on the adoption. One of the major challenges during the research and development processes is leakage of crucial patient data that can be used for malicious purposes.

Protection of crucial data – Another challenge is to ascertain that only the authenticated and most updated version of patient information/diagnosis data is made available to different parties during different phases of care.

Data governance, privacy, and security – By storing data across its network, blockchain technology eliminates the risks that come with data being held centrally but compels renewed focus on data governance with greater sensitivity to data privacy and security. From medical record to insurance claims to personal payment information, a lot of highly sensitive and heavily

regulated information flows through healthcare providers' systems. Cyberattack outages, breach notification and penalties, public trust, and even patient safety are primary concerns. Protecting the privacy and security of data is only possible when it is properly governed. For these reasons, and to optimize business processes, providers must focus on formalizing master data governance, establishing data standards and policies to sustain quality.

End user buy-in is essential for success – The educating of industry professionals and influencers to help educate the end users can prove challenging, as regulatory burden and shifting enforcement will complicate reporting and risk management.

Healthcare sector convergence - Margin and market pressures will drive further mergers and acquisitions (M&A) activity and horizontal integration of healthcare facilities. Healthcare sector convergence (insurance, pharma, etc.) will intensify operating margin pressures. With waves of convergence disrupting the business and operational models of insurance firms, pharmaceutical companies, and health plans, the healthcare providers end up absorbing more risk.

Full suite offerings - Rising patient preference for full suite offerings under unified systems will require controlling enterprises to develop seamless end-to-end processes and controls, whether delivered in-house or via close-knit supplier/partner arrangements. Healthcare customers, notably Millennials, increasingly prefer one-stop-shopping. While healthcare providers may seek horizontal integration opportunities to achieve economies of scale, patients want convenience. They demand predictable pricing and clear coordinated billing and claims handling.

BYOD security and healthcare breaches – A recent healthcare professional roundtable (https://www.deloitte.com) found that although a majority of healthcare providers had defined procedures for securing devices, 46 percent admitted the policies are not being followed. In a similar fashion, roundtable participants agreed that device encryption should be a part of any BYOD policy but that encryption requirements were rarely enforced. One reason for the prevalence of healthcare breaches is the lack of organizational adherence to their own policies.

PHI and HIPAA compliance - Legal and regulatory issues will need to be addressed, such as ensuring that blockchain solutions involving protected health information (PHI) comply with HIPAA privacy requirements.

Accurate master data - Maintaining accurate master data will be challenging in the face of growing supply chain complexity, M&A activity, and complex enterprise resource planning (ERP) IT systems.

Horizontal integration and patient expectations – Patient-centred healthcare is becoming a more significant success factor in the design of integrated health systems. People are frustrated that healthcare delivery remains largely unchanged despite huge advances in other areas of their lives. Today we can do just about anything on a smart phone or online, but when it comes to healthcare, it is still hard to book a doctor's appointment online or get a prescription electronically. People want access to healthcare that is responsive and flexible as online shopping. However, blockchain technology alone cannot efficiently store and transact patient health records without accessing an external database via *Smart Contracts, Ethereum, and Oracles*:

> In order to efficiently store data, every blockchain server will access an external database via smart contracts or the implementation of oracles (external services that push necessary information into the blockchain, instead of having the blockchain servers pull the information from outside sources).[8]

Smart Contracts, Ethereum, and Oracles

Smart Contracts -[9]

A Smart Contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible. Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met. Ethereum is an open source blockchain project that was built specifically to realize this

possibility. The term "smart contract" was created in 1996 by computer scientist (and lawyer) Nick Szabo, in a blog post titled**,** Formalizing and Securing Relationships on Public Networks, and reworked over several years.[10]

With technology's current level of development, smart contracts can be programmed to perform simple functions. For instance, a derivative could be paid out when a financial instrument meets a certain benchmark with the use of a blockchain technology and Bitcoin enabling the payout to be automated.[11]

Ethereum **-**[12]

Still in its early stages, Ethereum has the potential to leverage the usefulness of blockchains on a truly world-changing scale. Three reasons why Ethereum is being more widely used are:

1. Increasing application uses
2. More companies adopting decentralized cloud-based applications
3. Increased usage of smart contracts

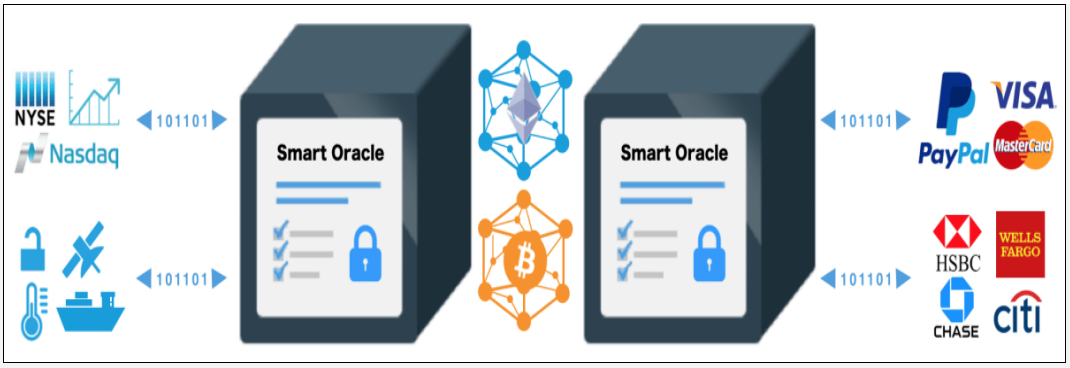
Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality. It supports a modified version of Nakamoto's consensus via transaction based state transitions. Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer.

Ethereum blockchain applications are usually referred to as DApps (decentralized application), since they are based on the decentralized Ethereum Virtual Machine and its smart contracts. Many uses have been proposed for Ethereum platform, including ones that are impossible or unfeasible. Use case proposals have included finance, the internet-of-things (IoT), farm-to-table produce, electricity sourcing and pricing, and sports betting. Ethereum is (as of 2017) the leading blockchain platform for initial coin offering projects with a market share greater than 50%.[13]

Oracles **-**[14]

Oracles, in the context of blockchain and smart contracts, is an agent that finds and verifies real-world occurrences and submits this information to a blockchain to be used by smart contracts. Smart contracts contain value and only unlock the value if certain pre-defined conditions are met. When a particular value is reached, the smart contract changes its state and executes the programmatically predefined algorithms, automatically triggering an event on the blockchain. The primary task of oracles is to provide these values to the smart contract in a secure and trusted manner.

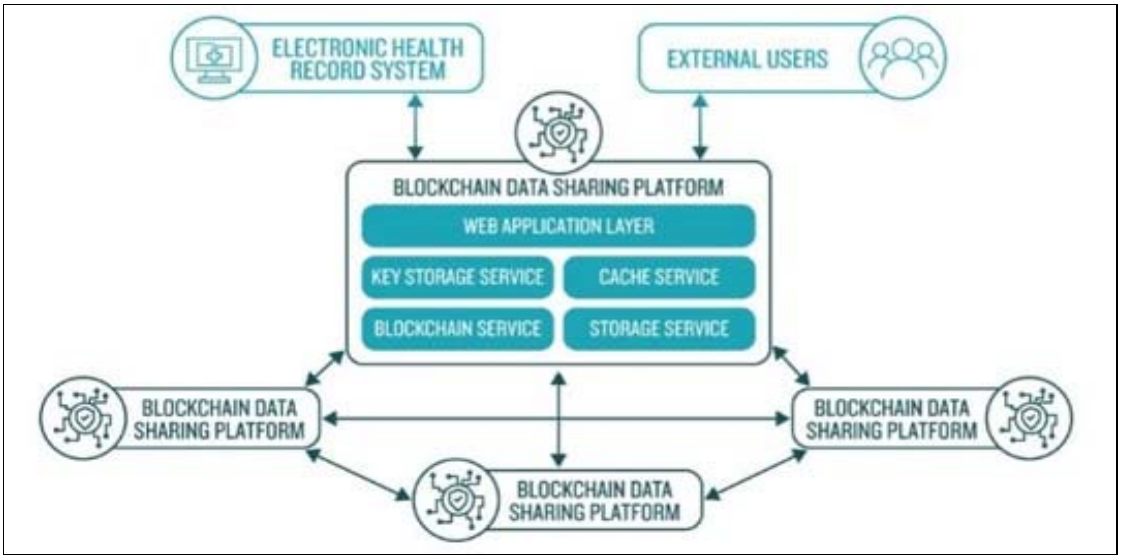
Blockchain cannot access data outside of their network. An oracle is a data feed provided by a third party service, designed for use in smart contracts on the blockchain. Oracles provide external data and trigger smart contract executions when pre-defined conditions are met. Such condition could be any data like weather temperature, successful payment, price fluctuations, etc. Oracles are part of multi-signature contracts where, for example, the original trustees sign a contract for future release of funds only if certain conditions are met. Before any funds get released, an oracle has to sign the smart contract as well.



According to Telehealth and Medical Today ™, blockchain has the potential to bring innovative solutions to the healthcare industry because, once entries are created on the chain, they are immutable, making blockchain ideal for storing permanent records:

> Our goal is to increase understanding of the potential of blockchain among subscribers to Telehealth and Medicine Today. Data stored in a blockchain is immutable and available

for access by separate parties. The excellent potential residing in this technology includes security, verification, and expanded data management for healthcare records, making it ideal for a new interoperability standard.[15]



Slowly but surely life science organizations are getting interested in this new technology. IBM already has a developed blockchain platform which provides developers with a number of simple industry use case scenarios for them to start their exploration. At this time, IBM provides use cases for supply chain, financial services, automotive, real estate, food safety, identity, and international trade, and they have expectations of adding use cases to fit the healthcare industry in the near future.

The interest in developing technological solutions that hold the promise to unite the disparate processes in the pharmaceutical industry and healthcare ecosystem, reduce costs, improve regulatory compliance, increase data flow, and improve patient experiences and outcomes has been ongoing. The transformative blockchain feature for health information exchange (HIE) lies in the ability to attach a standard layer of encrypted information to each record to protect all the data. Recently, the U.S. Food and Drug Administration (FDA) signed a two-year joint-development agreement with IBM Watson Health to explore using blockchain technology to securely share patient data for medical research and other purposes. The two

organizations intend to explore the exchange of health information from several sources, such as electronic health records (EHR), clinical trials, genomic data, and data from mobile devices, wearables and the internet-of-things (IoT). The initial focus will be on oncology-related information:

> "The healthcare industry is undergoing significant changes due to the vast amounts of disparate data being generated," said Shahram Ebadollahi, vice president for innovations and chief science officer for IBM Watson Health, in a release. "Blockchain technology provides a highly secure, decentralized framework for data sharing that will accelerate innovation throughout the industry."[16]

Starting blockchain projects for large enterprise adoption from scratch is difficult and could potentially burn through hundreds of millions of dollars, making it reasonable to assume healthcare leaders will turn to companies who already have developed blockchain service applications for answers. For example, Microsoft has program developers working on a number of projects, one of which is referred to as Azure Project Bletchley – Blockchain as a Service (BaaS) for Enterprise Solutions. Project Bletchley is a *middleware* toolset for developers that functions in the cloud supported by Azure. Azure is a comprehensive set of cloud services that developers and IT professionals use to build, deploy, and manage applications through a global network of datacenters.

The new building blocks of Microsoft's blockchain technology are so called *cryptlets* that can act as a smart contract surrogate that captures and executes an agreement on behalf of the transaction contained within the blockchain. Cryptlets can be used in smart contracts when additional functionality or information is needed and provided via a c*rypto delegate* or adapter.

Also important here are smart contracts on a ledger. These are simple software programs that run across all nodes in the network, and can extend the validation logic at each node, in a way that is automatable and undeniable. In the financial world, an example might be an insurance contract, or an offer to buy a share of stock in the future for a certain price set today. In

a healthcare setting, where a chain is being used to share personal data, it can be used to implement an authorization process and confirmation step that notifies the patient, or even places them in control, when their data is shared from one address to another.

Microsoft's approach to a global blockchain ecosystem is to build solutions to address real business problems. This is encouraging other tech giants such as IBM, Oracle, Hewlett-Packard, Samsung, and Amazon to deliver their own functionality that addresses shortcomings in the current blockchain offerings on the market.

Though the two most commonly cited examples of how blockchain can be used in healthcare are data interoperability and security, the stream of new possibilities is flowing as well. At the HIMSS17 symposium held in Orlando, February 2017, Tamara StClaire, a health IT advisor who previously worked as chief innovation officer at Conduent Health, formerly known as Xerox Healthcare, outlined several use cases, including master patient index, claims adjudication, supply chain and clinical trials. StClaire maintains that blockchain can be used to automate claim adjudication, such that the decision to deny or pay a claim is made without human intervention. All patient charges would be tracked and validated across different blockchain instances to see if everything for a patient has been done and where. There would be a better check and balance process to see what billing has been completed for a patient and who covered a patient for what. Medical billing errors, duplicate charges and fraud checks could happen in real-time as audits of medical codes happen, looking at codes like ICD-10 and CPT codes, as these codes would be part of the blockchain. As for clinical trials, StClaire states she believes the big advantage of using blockchain is to create a layer of de-identified data that researchers could tap to recruit patients. She made the case that the bitcoin-derived secure digital ledger technology could maybe offer the answer to an array of vexing healthcare challenges – not least of which is interoperability. "The current infrastructure is really inadequate to handle information exchange", she said. "Blockchain has the opportunity to impact those infrastructure challenges."[17]

To date, healthcare providers and allied personnel have been forced to cope using the software applications provided to them to function on a daily basis. These apps are basically inefficient with many data entry points that cause duplication of efforts collecting patient data, e.g. in hospitals there are multiple places in a patient record to enter something as simple as a patient date-of-birth and no real way to standardize that once it has been done. This problem could potentially be eliminated by tying patients to their data, rather than identity. Additionally, the interoperability and security potential of blockchain would enable a longitudinal health record by securing data as it is exchanged among organizations in a format that is usable for various clinicians across the care continuum. Rather than a central database, the blockchain record can be distributed and shared across networks, with credentialed users able to add to – but not delete or alter – the transaction log. Transactions are encrypted and must be verified by the network. "The software used to build a chain ensures that everyone on the network sees, validates, and confirms each proposed next block of data in the chain", Brian Behlendorf, executive director of Hyperledger at the Linux Foundation, explained in a blog post for HIMSS.[18]

Many sectors of the healthcare ecosystem can benefit from blockchain technology; the most important are listed here:[19]

1. Clinical Administrative & Backend	Scheduling, patient transfers, billing compliance

2. Medical Devices & Diagnostics	Monitoring, detection equipment
3. Doctor & Healthcare Service Search	Services to search for doctors, healthcare plans, and specialized healthcare
4. Doctor Network & Resources	Collaboration platform across hospitals and social networks that identify and share best practices
5. Electronic Health/Medical Records	Platforms for electronic medical charts, schedules, prescription tracking and referral letters
6. Gamification of Health	Gamification solutions for health and fitness
7. Precision Medicine	Genetic, metabolomics and epigenetic testing, analytic solutions, patient personalized reports
8. Healthcare Marketing & Campaign Management	Healthcare-specific customer relationship management (CRM) platforms
9. Healthcare Mobile & Communications/Messaging	Secure messaging for doctors, data sharing amongst healthcare professions
10. Supply Chain	Cold chain logistics, biobanking, drug shipping
11. Health Insurance & Payments	Health insurance marketplaces and platforms to manage and automate health benefits
12. Internet of Things Fitness (IoT)	Healthy eating trackers, exercise tracking wristbands, smartphone-controlled devices
13. Internet of Things Health Care	Glucose monitors, sleep trackers, pain relief wearables
14. Medical Big Data	Data management, solutions to normalize and link data across different systems, predictive

	analytics
15. Mobile Fitness/Health Apps	Fitness apps, mindfulness exercises
16. Nutrition Science & Advice	Symptom checklist, drug information, and resources that discuss more specific issues
17. Patient Engagement & Education	In-hospital multimedia systems, clinical trial recruiting, patient relationship management
18. Population Health Management	Population data management, coordinated care across populations
19. Remote Monitoring & Family Care Management	Services that provide caregivers to senior citizens, alert systems for in-home care
20. Telehealth/Telemedicine	Patients to doctor video conferencing, remote monitoring, remote diagnosis

Since all data is copied to every entity on the chain, confidentiality and privacy need to be carefully designed into the platforms. Furthermore, this widespread distribution means space is at a premium, so small data and metadata is preferred. So the way blockchain applications are designed is important. In healthcare very large files are often used, such as x-rays and scans. There is no need to store those entirely on the chain, but storing links to those as well as *hash* to ensure that it has not changed would likely be right.

There is a function in cryptography called a *one-way hash*, also known as a message digest, fingerprint or compression function. It is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence. Hash functions are the building blocks for modern cryptography. A hash function is a cryptographic algorithm which is used to transform large random size data to small fixed size data. The data output of the hash algorithm is called hash value or digest. The basic operation of hash functions does not need any key and operate in a one-way manner. The one-way operation means that it is impossible to

compute the input from a particular output. A basic use of hash function is to generate and verify digital signatures.

What is the cost of setting up a blockchain in healthcare?

Pricing to set up a blockchain is an anomaly because there are such discrepancies of adoption throughout the landscape of the healthcare industry. Since most existing systems are contained within private databases, migrating or rebuilding those systems on a blockchain requires very specialized coding knowledge and detailed architecture. A few large enterprises, like IBM and Oracle, are already putting together proprietary pricing models for large healthcare institutions, such as hospitals, but estimating costs would vary depending on the specifics of the project. For smaller and more medium size medical practices looking to migrate all of their data onto a blockchain, more service providers will use the monetized model of labor and technology to migrate those processes. This pricing model would be a combination of contract fees, hardware, and intellectual property.

Are you ready for a blockchain healthcare transformation?

Blockchain isn't a magic wand. As new business applications for blockchain emerge, your enterprise needs to ask challenging questions about reaping potential benefits.[20]

- Should we join in an existing blockchain network or create our own?
- What current business processes could most benefit from blockchain?
- What existing technical approaches to moving and integrating data into or out of a blockchain will be relevant to our use cases?
- Can we employ standards-based application programming interfaces (APIs) to simplify data transfer, application and network integration?
- Who are our technology and business partners, and how can we convince them to support a blockchain initiative to transform or even eliminate a given process?

Recent History and Looking Ahead

The hype around blockchain had reached new heights at HIMSS18 in Las Vegas this past March. Much of it centered on how an immutable, decentralized ledger of transactions and exchanges could be used to solve healthcare issues around interoperability and data sharing. Speaking at the conference, Jason Goldwater, MA, MPA**,** senior director of the CedarBridge Group LLC, having worked on quality measurements at both CMS and the National Quality Forum, suggested it could also streamline another headache for healthcare professionals: quality reporting. Goldwater said blockchain may not solve all of healthcare's problems, as other HIMSS sessions may have claimed, but he does believe it has the potential to revolutionize outcome measurements, both in how measures are gathered and how they are reported. The transition to value-based care, he argued, cannot rely on process-focused measures or siloed data. That is where blockchain comes in. "Then quality is not something that's measured at one point in time, quality is measured dynamically over time," Goldwater said. "You're making sure the patient is consistently receiving quality care and blockchain has the ability to capture information from such a wide variety of sources that the patient can send to the doctor, that it then takes out the two reasons why we haven't done this yet," which he said were provider burden and security concerns. By taking measurement at the time of the outcome, then giving patients the ability to send it to other providers, Goldwater said it not only makes sharing the data easier but can more easily identify what measures matter. [21]

Over the past two years, a crowd of startups has begun vying for a piece of the emerging healthcare blockchain market. Some, like PokitDok and Atlanta-based Patientory, plan to mine proprietary cryptocurrencies which investors can buy in lieu of stock, medical providers may earn as a reward for achieving better outcomes, and patients might score for meeting wellness goals or participating in clinical trials. (Patientory's initial coin offering, or ICO, raised more than $7 million in three days.)

Cryptocurrency mining, or cryptomining, is a process in which transactions for various forms of **cryptocurrency** are verified and added to the blockchain digital ledger. ... In order to be competitive with other cryptominers, though, a **cryptocurrency** miner needs a computer with specialized hardware.

What Is Cryptocurrency Mining? Webopedia Definition
https://www.webopedia.com/TERM/C/cryptocurrency-mining.html

Several fledgling healthcare-blockchain companies have found powerful corporate partners: Intel for Silicon Valley's PokitDok, Kaiser Permanente for Patientory, and Philips for Los Angeles-based Gem Health. At least one established provider network, Change Healthcare, is developing blockchain-based systems of its own. In January 2018, Change Healthcare launched what it calls the first *enterprise-scale* blockchain network in U.S. healthcare. It is a system to track insurance claim submissions and remittances. [22]

Accenture PLC is a global management consulting and professional services firm that provides strategy, consulting, digital, technology and operations services. They predicted as far back as 2014 that more than twenty-five million people, or approximately one in thirteen patients, will have their medical and/or personal information stolen from their healthcare provider's digitized records between 2015 and 2019:[23]

Two examples of Accenture PLC's 2018 predictions demonstrating how the digital world is changing people's habits and expectations are:

- *Prepare for a world of change* – Rapid technological advancements uproot the digital and physical experiences of our everyday lives and redefine our relationships with everything around us.
- *In transparency we trust* - In this world of decentralized ownership and tight security, blockchain has the potential to create transparency that will clear the fog of internet ambiguity.

Additionally, companies are increasingly enabling people, via technology, to build on opportunities that are both grand and granular. The power of the hyper-personalization that technology now makes possible drives goals both at the level of entire industries and the level of individuals. The digital leaders of the world are already starting their journey to make the big plays; Philips is looking to transform healthcare to a connected, comprehensive experience that is both intertwined and accessible throughout people's lives.

By empowering people with more human technology, doctors will transform the relationship they have with their patients. If patients are to be partners, and technology serves as the link to how healthcare providers will empower people, then the goal is to design technology that is both secure and works reliably. Enabling individualized health information on the blockchain is the transformational infrastructure for the creation of real-time precision medicine and for people to effectively reach their goals. These new partnerships will help the healthcare continuum to cement a place in the next-generation of healthcare in our society.

From the eyes of patients, connected healthcare is not an improvement because of the technology itself. The draw is the empowerment it gives individuals over their own health, in an industry long associated with impersonal interactions and untenable wait times. Because innovation is an inherently complex and dynamic social process, there is tremendous value in connecting theory and practice. Clinical research and health information data sharing are but ripples in a growing wave of reimagined applications of distributed ledger technologies beyond the digital marketplace for which they were originally created.

Companies like Philips and CVS Health are leading because their technology strategy focuses on the needs of the individual patient, on their terms. Through apps and connected devices that integrate into people's lives, these companies allow doctors and nurses to live alongside each patient, build a closer, more personal relationship, and provide comprehensive – not just reactive – care.

Distributed ledger technology is designed to securely maintain continuously growing lists of data records and transactions, and according to industry experts, it has the power to potentially transform healthcare as we know it. New technological trends fuel innovation, and blockchain is causing a hype and optimism that has rarely been seen in the history of technology. For example, the Institute of Electrical and Electronics Engineers (IEEE) is deeply entrenched in advancing a wide array of uses for blockchain in healthcare, as open innovation will play a key role in the developed economies over the next decade.[24]

The uptake of the technology could save the healthcare industry up to $100 billion per year by 2025 in data breach related costs, IT costs, operations costs, support function and personnel costs, counterfeit related frauds, and insurance frauds. One of the biggest beneficiaries of the technology will be the pharmaceutical companies that lose approximately $200 billion to counterfeit drugs each year.

Conclusion

The encryption in blockchain networks and the permissions that prevent data tampering and unauthorized access may hold the promise to secure and protect valuable patient data from breaches and improve overall efficiencies across all medical ecosystems, but the novel blockchain is not a complete cure-all solution just yet. There is still much work ahead as use cases to fit healthcare are still in the early stages of development, and moreover, the current absence of regulation needs to be resolved to address questions about how blockchains will be managed and run.

Unleashing blockchain's potential in healthcare on a widespread basis will require significant investment and efforts, including seamless integration with the current infrastructure, and blockchain providers may experience resistance from healthcare players for changing from legacy systems and processes to blockchain. Considering its greatest benefits revolve around streamlining the coordination among multiple providers, payers and patients, healthcare

organizations will have to agree to collaborate with external partners and stakeholders, including competitors.

Because blockchain promises to restructure how the healthcare industry conducts business, organizations can use this time to plan ahead and develop forecast budgets and implementation strategies, rather than adopting a wait-and-see approach. The time to start thinking, planning and work towards implementation by building proofs of concept, running pilots and organizing itself to take advantage of this revolutionary advancement in technology is now. By planning ahead, organizations and healthcare leaders will be in the position of influencing the development of blockchain networks and industry consortia, including the choice of participants and governance rules required to be successful in a blockchain-enabled world.

Key Words:

Blockchain, BYOD, Disruptive Technology, Distributed Ledger Technology, Horizontal Integration, Interoperability, Middleware, Open Source Technology, Oracles, Security, Smart Contracts

Abstract

Health management and administrative systems remain relatively untouched by technology and regulatory reform and stand ill-equipped to serve the current and future needs of their target population. This exploratory paper will focus on discovering why the new emerging disruptive technology known as *blockchain* is expected to be the next-generation healthcare solution, and why capitalizing on this technology has the potential to connect fragmented systems to generate insights and to better assess the value of care. Blockchain technology, while still nascent, is said to have untapped potential. This paper looks at both the potential benefits and challenges of adopting distributed ledger technology in healthcare, especially as it relates to interoperability, claims adjudication, supply chain and longitudinal electronic health records (EHR). While the perfect application of blockchain in healthcare seems futuristic, conversation around its potential must happen now. Given the speed of advancement in blockchain technology, healthcare professionals would be wise to closely track new blockchain-related healthcare applications as researchers' project that 55 percent of healthcare applications will have adopted blockchain for commercial deployment by 2025.

ILLUSTRATIONS

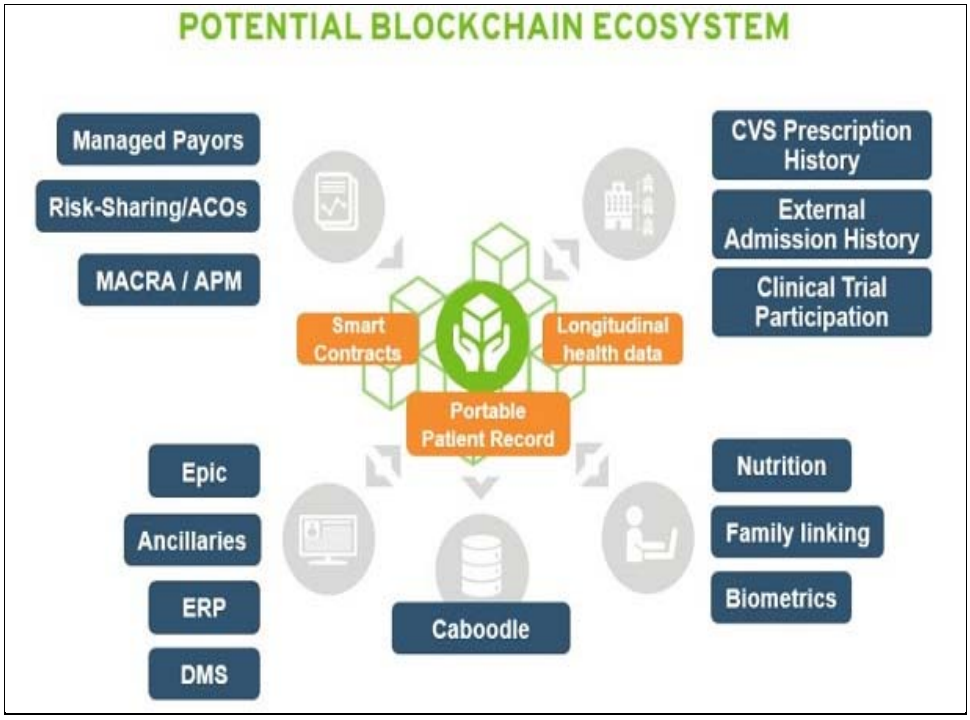


Fig. 1

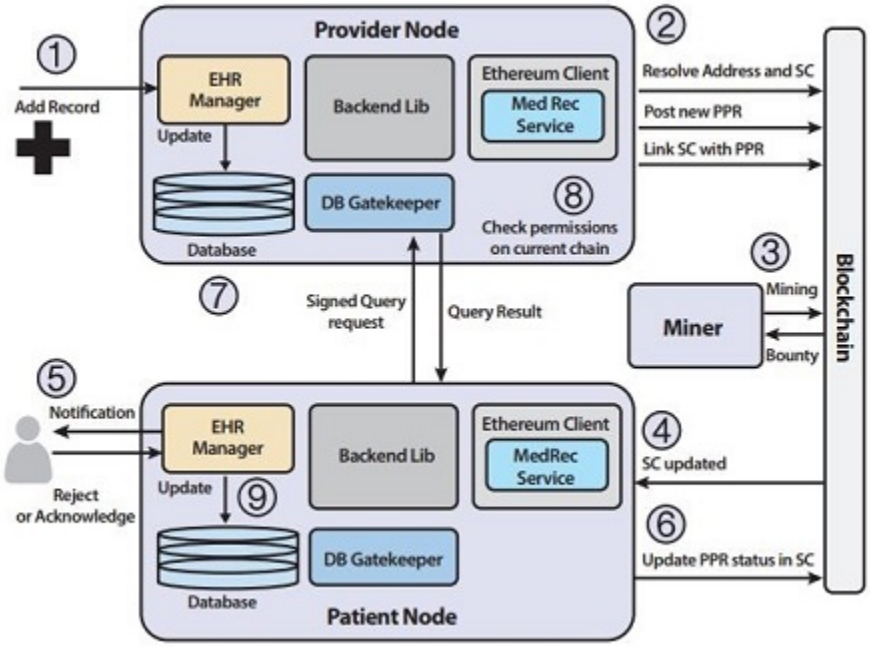
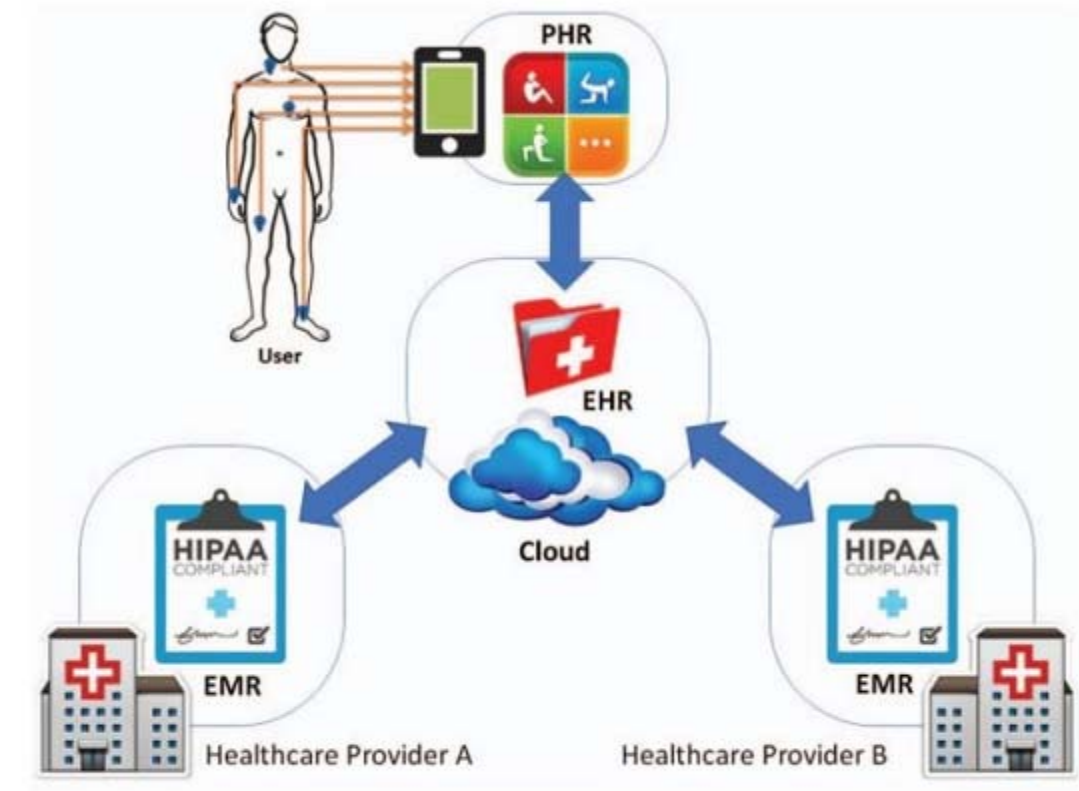


Fig. 2



Blockchain for your medical and health records: A conceptual cloud-based ecosystem for electronic medical and health records (EMR/EHR) and personal health records (PHR).

Fig. 3

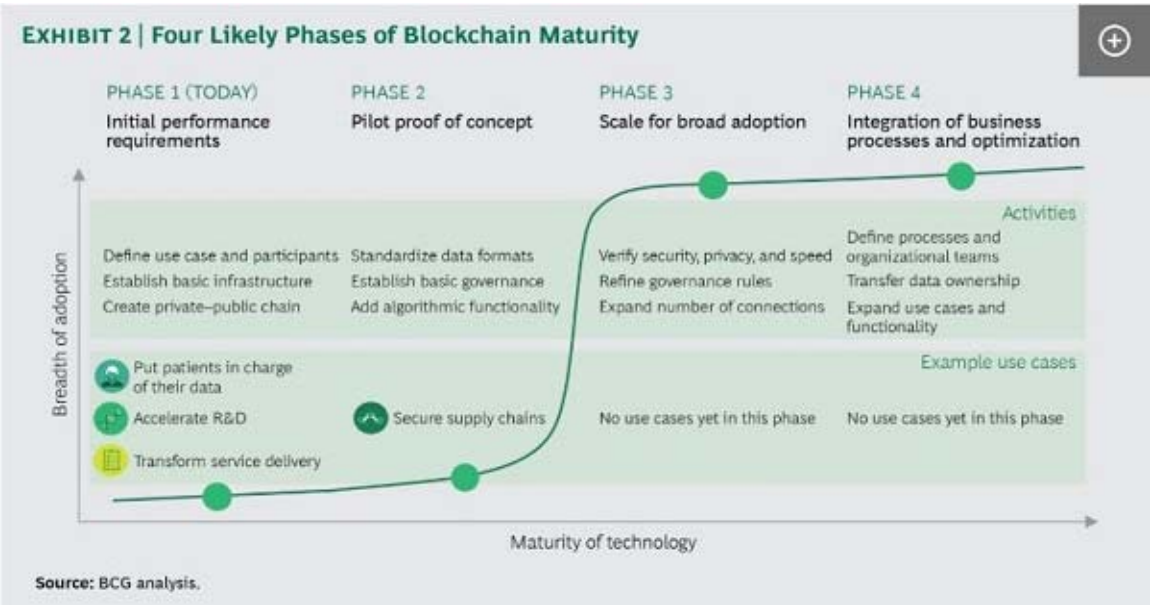


Fig. 4

Bibliography

Accenture. *Seven Predictions on Design and Innovation for 2018.* December 19, 2017. https://www.accenture.com/us-en/blogs/blogs-seven-predictions-design-innovation-2018.

Alhadhrami, Zainab, Salma Alghfeli, Mariam Alghfeli, Juhar Ahmed Abedlla, Khaled Shuaib. "IEEE Xplore Digital Library." *IEEExplore.com.* November 21-23, 2017. https://ieeexplore.ieee.org/document/8252043.

Bartlett, Jessica - Reporter. *IBM Watson Health Delves Into Electronic Medical Records via FDA Partnership.* June 11, 2017. https://www.bizjourals.com/boston/news/2017/01/11/ibm-watson-healthdelves-into-electronic-medical.html.

Czeschik, Christina and Ratko Stambolija. *A Guide.* Herkulesstr.3-7: Intellicore UG (haftungsbeschrankt), 2017.

Elton, Jeff and Anne O'Riordan. *Healthcare Disrupted: Next Generation Business Models and Strategies.* Hoboken, New Jersey: John Wiley & Sons, Inc., 2016.

Firth, Shannon. *CMS Projects U.S. Health Spending to Reach 19.9% of GDP by 2025-But estimates don't account for potential changes in ACA.* February 15, 2017. https://www.medpagetoday.com/publichealthpolicy/healthpolicy/63176.

Gregory, John. *How blockchain could improve quality reporting.* March 26, 2018. https://www.healthexec.com/topics/quality/himss18-how-blockchain-could-improve-quality-reporting.

Hamilton, Booz Allen. "Blockchain as a Foundation for Sharing Healthcare Data." *Blockchain in Healthcare Today*, 2018: 12.

IBM. *Transform healthcare outcomes with the simplicity of IBM Blockchain.* 2018. https://www.01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=KU912407USEN.

Leroux, Darren (/author-darren-leroux). *Healthcare IT News.* August 12, 2014. https://healthcarenews.com/blog/heathcare-byod-challenges (accessed January 12, 2018).

Magazine, Healthcare Information. "https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-accounted-45-all-ransomware-attacks-2017." *Healthcare-Informatics.com.* 2017.

Miliard, Mike. *Blockchain's potential use cases for healthcare: hype or reality?* February 22 2017, 2017. https://www.healthcareitnews.com/news/blockchains-potential-use-cases-healthcare-hype-or-reality.

—. "How Does Blockchain Actually Work In Healthcare." *Healthcare IT News.* April 13, 2017. https://www.healthcareitnews.com/news/how-does-blockchain-actually-work-healthcare.

Miller, Kenneth. "Will Blockchain Technology Usher in a Healthcare Data Revolution?" *Future Frontiers*, March 2018: 5.

News, CCN. "This Blockchain Platform Aims to End Healthcare Data Breaches." November 9, 2017. https://www.ccn.com/platform-brings-end-patient-data-breaches (accessed January 12, 2018).

Obey, David R. *H.R.1-American Recovery and Reinvestment Act of 2009.* Feb 17, 2009. https://congress.gov (accessed April 10, 2018).

Redcar, Michael. *Blockchain & Healthcare.* Amazon Kindle Edition, 2017.

Roethke, Jon and Hunter Gebron. *A Story About Smart Contracts.* MetaX-Publications, n.d.

Saric, Alex. *Chief Marketing Officer, Ivalua.* Becker's Health & CIO Report, 2018.

Schumacher, Axel PhD. *Blockchain & Healthcare, 2017 Strategy Guide.* 2017.

Sharda, Pallav. *Before Disrupting Healthcare: What Innovators Need To Know.* Pallav Sharda, 2016.

Shen, Lucinda. *Blockhain Will Be Used By 15% of Big Banks By 2017.* September 28, 2016. https://fortune.com/2016/09/28/blockchain-banks-2017.

Szabo, Nick. "Formalizing and Securing Relationships on Public Networks." *Satoshi Nakamoto Institute.* 1997. https://nakamotoinstitute.org/formalizing-securing-relationships/.

Tapscott, Don & Alex. "What is Blockchain Technology? A Step-by-Step Guide for Beginners." *Blockgeeks.com.* 2016. https://blockgeeks.com/guides/what-is-blockchain-technology.

Endnotes

[1] CCN News, "*This Blockchain Platform Aims to End Healthcare Data Breaches",* November 9, 2017, https://www.ccn.com/platform-brings-end-patient-data-breaches/

[2] Darren Leroux, (/author/darren-leroux),"*Health BYOD Challenges",* Healthcare IT News, August 12, 2014, https://www. healthcareitnews.com/blog/healthcare-byod-challenges

[3] Alex Saric, Chief Marketing Officer, "*Balancing HIPAA regulations, patient care and cost in 2018"*, Ivalua/ February 12, 2018, *https://www.beckershospitalreview.com/healthcare-information-technology/balancing-hipaa-regulations-patient-care-and-cost-in-2018.html*

[4] Mike Miliard (/author/mike-miliard), editor, Healthcare IT News, April 13, 2017, www.*Healthcareitnews.com/news/how-does-blockchain-actually-work-healthcare*/

[5] Kenneth Miller, *"Will Blockchain Technology Usher in a Healthcare Data Revoluation"*, Future Frontiers Feature Story, March 27, 2018, https://leapsmag.com/will-blockchain-technology-usher-in-a-healthcare-data-revolution/

[6] Lucinda Shen, *"Blockchain Will Be Used By 15% of Big Banks By 2017",* September 28, 2016, *http://fortune.com/2016/09/28/blockchain-banks-2017/*

[7] Shannon Firth, Washington Correspondent *"CMS Projects U.S. Health Spending to Reach 19.9% of GDP by 2025- But estimates don't account for potential changes in ACA"*, February 15, 2017, MedPage Today, https://www.medpagetoday.com/publichealthpolicy/healthpolicy/63176

[8] Christina Czeschek & Ratko Stambolija, "*A Quick Guide To Blockchain In Healthcare - How Can the Blockchain Be Applied To Healthcare?*", Intellicore Press, June 2017

[9] Smart Contracts: Blockgeeks.com, *http://blockgeeks.com/guides/smart-contract/*

[10] Jon Roethke and Hunter Gebron, "*A Story About Smart Contracts",* MetaX-Publications, Unlocking the blockchain for digital advertising, January 9, https://medium.com/metax-publications/a-story-about-smart-contracts-736497541e4d

[11] Don & Alex Tapscott, "*What is Blockchain Technology?*", A step-by-Step Guide for Beginners, Blockchain Revolution, 2016

[12] Ethereum: Blockgeeks, *http://blockgeeks.com/guides/what-is-ethereum/*

[13] Ethereum, Wikipedia, https://en.wikipedia.org/wiki/Ethereum

[14] Oracles: Blockchainhub, *https://blockchainhub.net/blockchain-oracles/*

[15] Telehealth and Medicine Today ™, Blockchain HIE Overview*: "A Framework for Healthcare Interoperability"*, https://telehealthandmedicinetoday.com/index.php/journal/article/view/25

[16] Jessica Bartlett – Reporter Boston Business Journal, Healthcare, *"IBM Watson Health delves into electronic medical records via FDA partnership"*, (Bartlett 2017), published June 11, 2017, https://www.bizjournals.com/boston/news/2017/01/11/ibm-watson-healthdelves-into-electronic-medical.html

[17] Mike Miliard, WTN News – HIMSS17, *"Blockchain's potential use cases for healthcare: hype or reality"?,* by Healthcare IT News, published February 22, 2017, https://www.healthcareitnews.com/news/blockchains-potential-use-cases-healthcare-hype-or-reality

[18] Brian Behlendorf, Executive Director of Hyperledger at The Linux Foundation, "Blockchain 101 for Healthcare" HIMSS 2018 Conference & Exhibition, March 5-9, Session 145/March 7, 2018, http://365.himss.org/sites/himss365/files/365/handouts/550919914/handout-145.pdf

[19] Axel Schumacher, PhD, "*Reinventing healthcare: Towards a global blockchain-based precision medicine ecosystem*", Blockchain & Healthcare 2017 Strategy Guide

[20] IBM: Transform healthcare outcomes with the simplicity of IBM Blockchain, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=KU912407USEN

[21] John Gregory|Quality, "*How blockchain could improve quality reporting*", Healthcare Exec, March 26, 2018*, https://www.healthexec.com/topics/quality/himss18-how-blockchain-could-improve-quality-reporting*

[22] Ibid, Page 7

[23] Accenture, "*Seven Predictions on Design and Innovation for 2018",* Accenture Career Blog, December 19, 2017, *https:\\www.accenture.com/us-en/blogs-seven-predictions-design-innovation-2018*

[24] Zainab Alhadhrami, Salma Alghfeli, Mariam Alghfeli, Juhar Ahmed Abedlla, Khaled Shuaib, IEEE Xplore Digital Library, "*Introducing blockchain for healthcare*", 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA, 21-23 Nov. 2017), *https://ieeexplore.ieee.org/document/8252043/*