Chapter 2
Digital Transformation of Healthcare

Hamid Jahankhani and Stefan Kendzierskyj

Abstract The digital transformation needs to go a lot further to provide a seamless but secure and protected data interchange where a multitude of beneficial impacts can be gained such as longitudinal medical data, interoperability, secure patient centric generated data and its use cases, to name a few. Positioned with the increasing threat of data breaches, the healthcare sector has started to make deeper inroads into the beneficial uses of blockchain as the mechanism to provide immutability, audit trail, security and protect the privacy of data to ensure a better way forwards for healthcare transformation. This chapter aims to discuss the impact of digital transformation on the healthcare industry.

Keywords Digital transformation · Interoperability · Blockchain · IoMT · Data breaches · Cyber-attacks · Patient centric data · Electronic health records · Health information exchange

2.1 Introduction

The healthcare industry has undergone a transformation, as other industries, with the move from paper based methods to electronic and technology moving more from on-premise to cloud based servers with some levels of integration to other systems. But looking further into the current setup and future needs, it is clear a much more strategic digital transformation needs to happen for a number of reasons that all support and benefit each other's case. This expeditious progression in technology is leading towards more precision based medicine with better patient outcomes at point-of-care. This helps both healthcare professionals and patients to arrive at more efficient and quicker diagnosis. Technology is assisting this movement forwards be it in smart wearable devices, IoMT, etc., but a transformation is needed to see more widespread interoperability between the silos and disparate

H. Jahankhani (✉) · S. Kendzierskyj
London Campus, Northumbria University, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk; Stefan.Kendzierskyj@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_2

systems. An individual patient's medical record still sits in an insular system with no full archive of the longitudinal medical history. Also, even though it is well documented that the healthcare industry is under cyber-attack and processes/solutions are continually deployed to mitigate the attacks, it still has not lessened the fact that data is widescale breached. As all technology progresses at fast rate of knots then some form of methodology is needed to ring-fence the security aspects, keep integrity but equally provide transparency of data.

Blockchain appears to be the driving mechanism to offer a secure framework to operate under and enables the possibility to provide this needed interoperability and help progress the transformation in a more integrated nature. The themes associated with transformation can all benefit from this programme of enhancement leading to possibilities to make better use of artificial intelligence and machine learning for more precision based medicine and better delivered patient outcomes.

2.2 Defining the Driving Factors of Blockchain in Healthcare

The focus of this section discusses the advocacy of blockchain in healthcare and for a number of important reasons that stand independently of each other, but collectively create a strong purpose to solve legacy and more recent issues, some causing more serious effects. Transparency and security of data are key drivers that blockchain can provide and take care of the corruption, fraud, misconduct that are discussed in Chap. 3 in how clinical trials are conducted. Closely linked, are improving patient privacy and having a more patient centric outlook for a longitudinal medical history that solves interoperability problems.

Figure 2.1 presents the healthcare landscape and starts with current issues and working counter clockwise to the blockchain mechanism.

The above mapping explains the current issues with the disparate silos of data that offer no linkage or ease of data access to patients, health providers and other organisations. Although held in silos this does not offer any confidence in privacy and security of patient data since there may be inadequate layers to offer correct authenticated access. There are a lot of benefits to hold the medical records in what is known as longitudinal data giving patients and healthcare providers a complete medical history. Also, with all this longitudinal medical data held in a secure method such as blockchain gives rise to great opportunities of analytics, with the consent of parties involved. Consent can be authenticated via blockchain. These analytics can offer a greater insight into health issues and better ways to offer more efficient clinical paths and form a validated health information exchange that takes care of interoperability issues.

Alongside longitudinal medical data are other important considerations regarding clinical research data and the process/current methods deployed from setting up trials, ensuring correct stages of informed consent are captured, to the reporting in the trials and post marketing of drugs. Issues arise in a number of stages with evidence in how trials are setup, non-conformance of consent and the dangers of

Fig. 2.1 Mind map of all concepts connected to the healthcare landscape

selective reporting, bias and misconduct which leads to much more serious implications explained in later sections. Blockchain can play a significant part in all parts of clinical research processes.

The advancement of smart wearables and Internet of Medical Things (IoMT) has meant much more accurate data can be captured seamlessly as sensors update cloud systems automatically. There is a huge increase in data expected with the billions of medical devices set to occur over the next few years. More data presents some concerns over storage with the cost implications but equally over the security of the data. Again, with some application to blockchain there can reside a more secure method to authenticate access to the data to only those with permissions that were allowed. This will give more clarity and privacy comfort to patients knowing that authentication is the layer of protection to their sensitive medical data.

As the Fig. 2.1 map illustrates that there is a very alarming factor indicating the rise of cyber attacks in the healthcare section and their sophistication. It's a known fact that the healthcare industry suffers the highest level of cyber-attacks. These attacks result in a multitude of issues from ransomware and data breaches that lead to identity theft and victimisation. Some attacks can be devasting and after effects

not fully understood since patients will not likely be aware of any criminalisation of medical data post attack from the breached data. Clearly, the reasons for some undertaking the attacks are financial gain from selling of the breached data at high values in comparison to other data such as credit card information to obtaining ransomware payments and further spiralling effects of identity theft. But hacktivism is also on the rise where financial gain is not the motive and more born out of a desire to install chaos or state sponsored attacks designed to destabilise economies or political turmoil. Exposure to the increased cyber-attacks in healthcare is a serious issue, not just for the healthcare organisation but also to the individual, since none can determine what damage can be achieved with breached data in the hands of criminals. It is a driving factor to ensure a method is cultivated to protect and secure such as blockchain.

The following other sections in this Chapter covers areas of healthcare transformation such as IoT, smart wearables, devices, etc., that enhance aspects of precision medicine and patient outcomes but create the additional concerns with more data and the way it is currently. More depth is given to the interoperability that blockchain provides and higher levels of protection for privacy of data than the current methods of Trusted Third Party. Figure 2.2 displays some of the central themes of healthcare transformation.

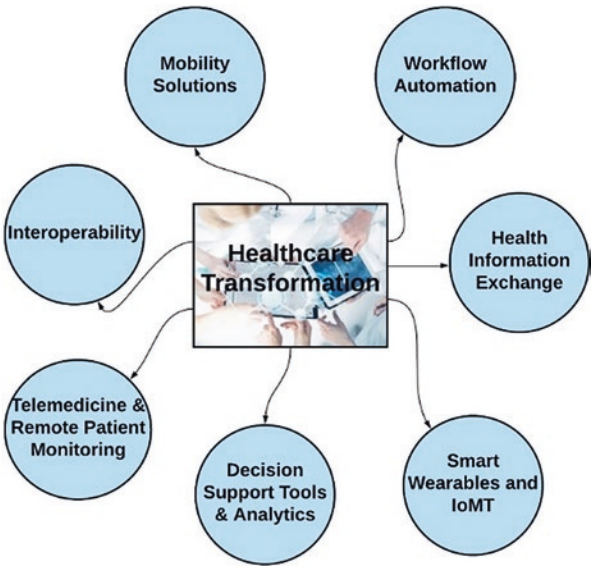

Fig. 2.2 Healthcare transformation drivers

2.3 Digital Transformation of Healthcare Records

All the population in any given territory, at points of their life, touch with healthcare records. There has to a place where all the patient's medical history and clinical data is stored. The obvious key data is what makes our identity unique, be it data of birth, social security number, and so on. It also contains all the diagnosis, medications, allergies, immunizations, laboratory test results. So, a mixture of personal and highly sensitive information. It is clear why medical records are intrinsic to the operational side of healthcare as without access to a record many functions would cease e.g. an operation due to take place needs have the medical record reviewed first. The records will contain extremely sensitive information that will have direct correlation to how they should receive treatment and diagnosis, Dubovitskaya et al. (2017). The records are also shared between many parties that needs give input/opinion as to arrive at best outcomes.

Personal and sensitive information makes the value of a healthcare record be worth a much higher premium on the deep web. This is due to personal identity information being something one cannot just cancel as would happen with a stolen credit card. The criminalisation value also increases in terms of its re-use life cycle or longevity, so the more times it can be re-sold or help to purchase medications, setup other criminal ventures, etc. So, the digitalisation of records has made it easier to re-use since when cyber-hackers attack they can access many records quickly, remotely and in a format that is easily transferable to the deep web or other criminal exchange sites. This was not the case or that easy with manual paper based records and would have been a laborious task for determined criminals.

In 2008, there were only less than 10% of medical records being stored in electronic format (see Fig. 2.3 and adoption of EHR records, ONC 2016).

With the obvious drawbacks of paper-based records, electronic healthcare records (EHR) increased to a point where practically all are kept in this format.

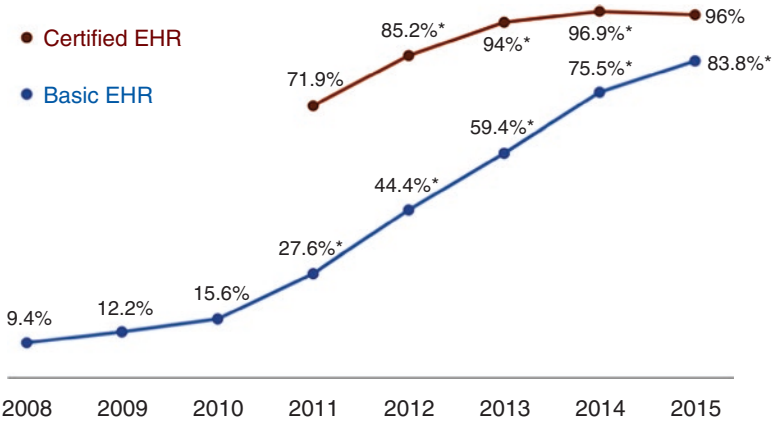

Fig. 2.3 Adoption of EHR records. (ONC 2016)

Whilst all acknowledge that paper-based records are difficult to share, the electronic format has largely been a similar issue and remained in silo providers and consequently this conveys an interoperability obstacle. This disparate updating of electronic medical records makes this difficult to track and keep up to date since they are held in silos and require multiple consents. All medical stakeholders need access and there is a case for the patient to also have assurances to access a longitudinal medical history. The transformation from paper to electronic was a necessary step and certainly the digital format allows a number of benefits in storage and ease of access. The issue lies in the interoperability and authentication as explained by recent organisations undertaking reports and analysis. Centralizing records is not the question or task but there is a question mark over its security when centralised as explained in later sections. Patients have concerns now in how the EHR is maintained with so many recent highlighted cyber breaches and this has impacted on their reluctance to divulge all information on the record.

In 2015, a published report by the Office of the National Coordinator for Health Information Technology (ONC) laid out the *Shared Nationwide Interoperability Roadmap* which presents a 10-year roadmap for interoperability, ONC (2015). In summary, 16 key areas were highlighted to find better ways to improve authorization/access, longitudinal health data, identity, etc., to name a few. As well as interoperability, this sensitive data would benefit all if it could be shared with a range of providers such as healthcare institutions, pharmaceutical industry, insurance companies, research establishments, gathering and securing of IoMT smart/wearable data, etc. But essentially the consideration is to put the patient first and give them the control and permission to allow access. From a patient perspective, giving them control through permissions is safer for allowing sensitive data to be accessed and clinical researchers have more benefits to gain permissions to a pool of data; whereas currently there are concerns in the way data is held in the centralised manner.

This has been the reason why there is great hope and consensus to create data access through blockchain architecture which contains the properties to be immutable, auditable, scalable, and ensure privacy and security are respected. As Dubovistskaya et al. (2017) note that it was relying on centralised entities storing sensitive data and controlling permissions (i.e. the patient had no control) that meant a single point of failure was an issue and the breakdown of any interoperability taking place. Also, why this discussion covers healthcare data breaches/ransomware as it's a significant added factor to give weight to the blockchain debate in terms of enforcing a better method of security.

Engelhardt (2017) in the review *'Hitching Healthcare to the Chain'* makes four concise points that summarise why healthcare needs balanced patient care with privacy/access, completeness of information, cost and by putting the patient at the centre of all in terms of data control allows them to be 'active agents in their own care'.

2.4 Privacy of Data and Interoperability

Data privacy has become more complicated as the increase of the Internet usage and digital/electronic data became a normal way to interface with holding records. Hence, why this has led to more recent need to control who has access to the data and regulated frameworks, such as GDPR. Since this publication has a central theme of securing data, then there are a few worthwhile factors to mention on how to treat the data depending on the healthcare requirements in the concept of blockchain. There are ways in which data could interact with blockchain, be it off-chain and on-chain data storage. Depending on its healthcare use case may be how data can be stored, if for example as off-chain in data lakes with blockchain acting as the authentication mechanism.

Essentially, for privacy permissions, there are three ways to store the data:

- **Unencrypted data** – all those on the chain, such as a public chain, can read all data
- **Encrypted data** – participants must use their private key to access the data
- **Hashed data** – this is the authorisation link that is the immutable digital record and timestamp and directs to where data is secured off-chain.

Sensitivity and who should access are the primary questions to help determine type of blockchain and how the data should be treated. Particularly in the healthcare industry, to comply with regulatory complications and the size of data (for example large data files such as imaging data) it is mostly likely to suit as off-chain deployment; Engelhardt (2017). In some cases, the data is being stored in data lakes, so an ecosystem is created with blockchain controlling as the hashed authentication permissions and pointing to the off-chain data lake. Linn and Koo (2016) explains that transactions in the block contain the user's unique identifier, the encrypted link to the health record and transaction timestamp. There can be certain metadata included within the transaction. Regarding the data lake, any information located here is encrypted and so protects only those authorised to access and security and privacy are respected.

See Fig. 2.4 for an example concept on the interoperability of healthcare data and how this ecosystem can facilitate a health data interchange in a secure way and protect privacy. In a later Sect. (2.4), *Is Healthcare Ready for Blockchain*, there are a number of successful pilots/live systems deployed that has given confidence to pursue further blockchain methods in healthcare.

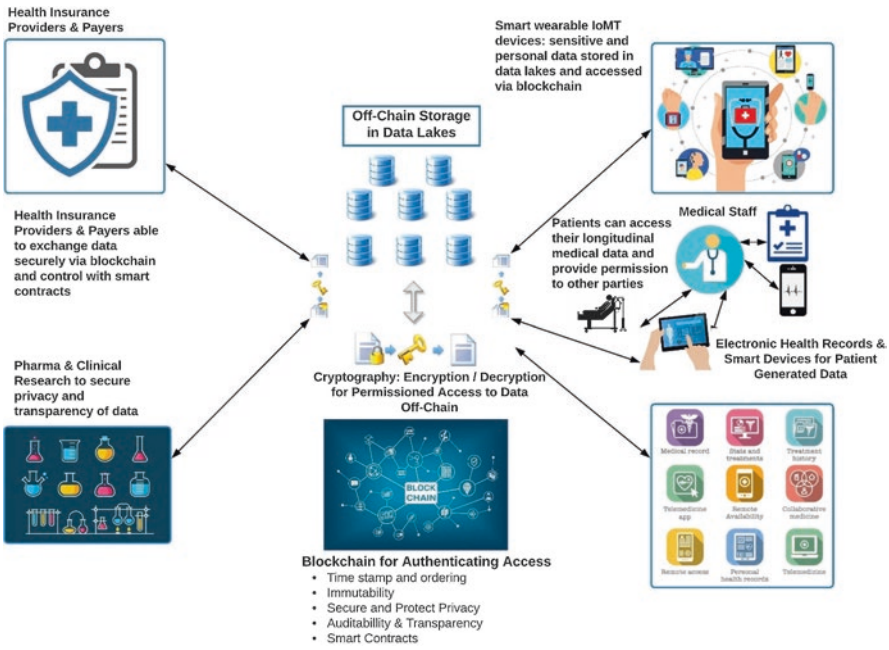

Fig. 2.4 Example of Blockchain ecosystem demonstrating interoperability and health data interchange

2.4.1 Interoperability

If privacy is a key component to a patient's security and how that data is authenticated through blockchain, then so too is the interoperability and how to overcome the disparate silos of data that presents to aim for the concept of longitudinal medical history. It is not just to satisfy the purposes of ease of access to medical history, but this is what is needed to also facilitate and keep up with the technological advances being made in precision based medicine. So, it is a fundamental aspect as part of healthcare transformation.

Interoperability covers the capability to allow a seamless interchange of data across different information systems and different software applications. Although operating systems and cloud based architecture have allowed a lot of flexibility it stops at the point where data cannot reach outside its silo unless organised in a requested way for particular information or setting up some form of API (Application Programming Interface) which means a method or pre-set protocols and programming. Although an interchange of information occurs, it is restricted in its requests, security and certainly a patient has no control over it. Plus, there is an expense, for example, to handle a requested transfer of patient information from one institution to another. If the expense was approved, then it too must satisfy the legal and regulatory side of things which likely has to have some stages of approval to send and add

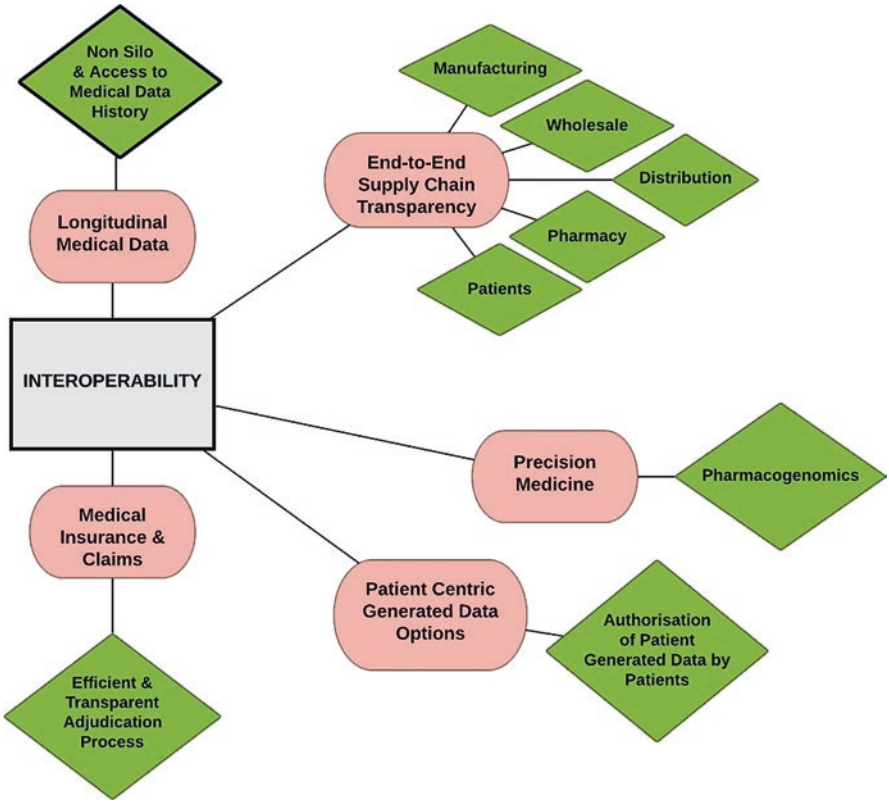

Fig. 2.5 Example of Blockchain ecosystem demonstrating interoperability and health data interchange

to delays and expense in time spent by various parties. This is exactly how blockchain can sit in the layer as the facilitator to all requests and be done through an automated but secure process. The requests could come from any permissioned entity/person that requires the information. As the blockchain authenticates the enquiry the transfer can all be tracked, timestamped in an immutable manner and work as smart contracts basis. This could be a pharmaceutical company requesting data sets across agreed patients to help develop drugs, medical claims could be settled faster, manufacturers trying to develop precision based medicine, etc. The list can be exhaustive and refer to Fig. 2.5 for how interoperability facilitates this and main theme areas of interest.

Perhaps, also a useful driver to transformational change is that, with regards to all the existing systems/databases, they do not need to be changed and can be enhanced and supported into an integration to blockchain architecture that is put in place. In some ways this gives the expression commonly used as requiring a 'single version of the truth' and certainly blockchain can offer that.

2.5 Pushing the Barriers of EHR Access

Currently there are many obstacles for allowing transfer of electronic healthcare records, if considering not just different providers, but also inter country requests as these likely have to satisfy country's legal regulations. These barriers create the difficulties for even a patient requesting their own medical data and there is a general unwillingness for providers to allow it or suggest a high expense to facilitate. Working in tandem to the difficulty to release records is also the concern a patient has in how secure their medical data is, so sometimes data from a patient is withheld due to sensitivity they feel could make then vulnerable should data be 'leaked' in an unauthorised way (it would be hard to track down due to no immutable process).

Blockchain can eliminate these barriers, allow the secure interchange of data to occur in a tracked and authenticated fashion and allow patients to trust the privacy blockchain provides (so perhaps be more transparent in what they advise their medical providers). There are already specific projects to transform how EHR can be better placed in a decentralised system such as blockchain. For example, Labchain is run by DDQ a company legally approved by the Dutch government to run a permissioned blockchain to allow digitally transferring blood values instead of the current system of using postal mail to exchange values, Labchain (2018). These would be blood analysis results that can be exchanged between hospitals and is secure as the data is not stored on the blockchain and is off-chain. This is used as authentication by way of hash values and is the digital fingerprint and immutability that blockchain can offer.

2.6 Smart Wearables and Data Capture

The possibilities and coming transformations within healthcare for using the Internet of Things (IoT) and Internet of Medical Things (IoMT) offers huge potential with remote monitoring and obtaining data from medical sensors on the body that report data seamlessly to cloud systems. Under older methods, biometric details would need to be physically captured or extracted from patients and written up as recorded information alongside the medical record and stored in a silo method. With the transformation of device capability and huge growth in the healthcare industry gives way to a more accurate and reliable method to record vital signs, skin temperature, body weight, heart rates, blood sugar levels, sleep patterns, calorie measurements, medication intake and effects, etc. There are also a whole range of fitness devices that offer metrics and analysis and offer a unique footprint for digital forensics explained in later chapters and shown in Fig. 2.6 as to types of devices and information exchange.

There are many benefits to improve patient outcomes, help conduct research and capture data in clinical trials. Rifi et al. (2017) observe these benefits and acknowledge the data sharing will improve the communication between patients and

Fig. 2.6 Smart wearable devices and interaction with patients and data storage off-chain

healthcare professionals, but also make aware that the security needs to be taken care of and blockchain is a solution to help provide this.

A robust infrastructure must be in place to protect and secure data; Liang et al. (2017) discusses the concept of data sharing and incorporating smart wearables into this design and running this over blockchain. Rather than just support the data in conventional cloud based systems in an uncoordinated or unconnected way this could be better addressed by using blockchain as the underlying architecture to control permissions, security and authentication. Whenever the patient generates health data it can then be seamlessly uploaded to the blockchain. It offers the quality of immutability and time-stamping, so for example in the case of clinical trials it's of importance to capture valid and correct data from smart wearables, otherwise it will be difficult for researchers to correlate and measure. Also, looking at it from the perspective of a patient it provides that protection and security layer to the personable and sensitive information a patient would be concerned if breached into places where identity theft and victimisation are the currency of criminals. As explained later in this chapter there are a few innovative live deployments where patients can make use of their data accumulated from their medical interactions. For example,

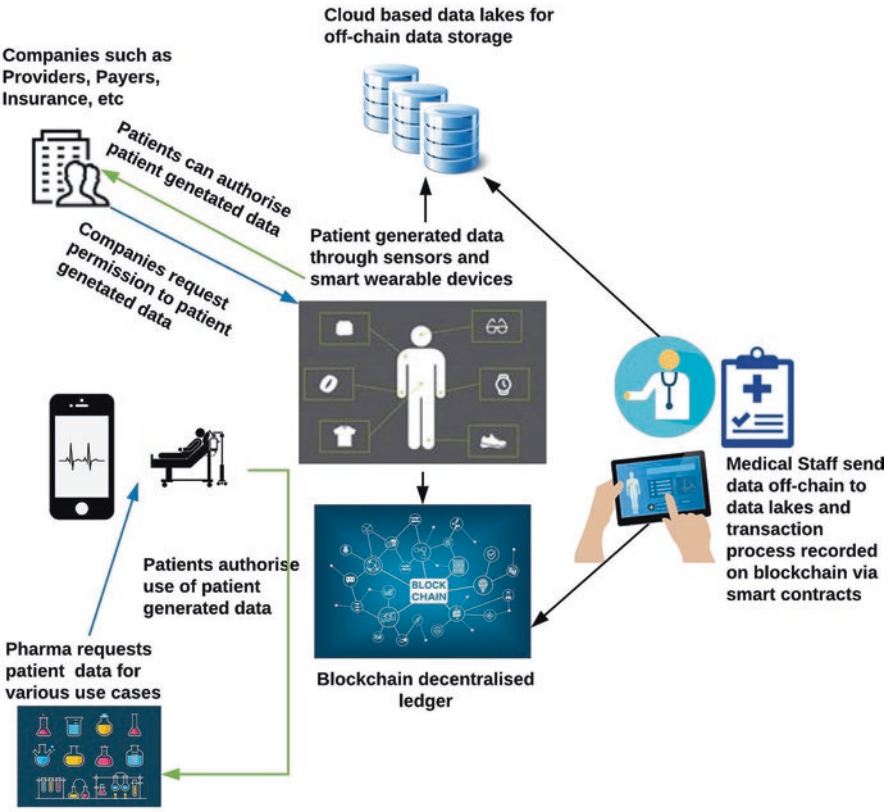

Fig. 2.7 Patient Centric Personal Health Data Sharing

either selling or donating biometric data to pharmaceutical industry. What was once a model where the patient was the last to know on contents of their data (or what was held on them) or be able to access data puts them in a position of control in this patient centric model. It ties very closely in with interoperability regarding data and its access points.

The idea of patient centric generated data, where the patient is at the centre of how their data is utilised, can be seen in Fig. 2.7. It gives a concept flow of the patient being in control and experience a better range of outputs than current architectures allow.

Looking specifically inside the world of clinical research, accuracy and transparency are key indicators to help measure effectiveness in trials. Zevala (2017) adds weight to the reasons why smart wearables are helpful for improving accuracy in clinical trials with data being collected in between visits instead of manual processes and relying on memory of patients. This also takes care of data becoming corrupted and can also alert researchers to any non-compliance or safety issues to the patient. Also, as the data is automatically collated this offers flexibility to the

patient and not impact on their time regarding reporting/recording. Bresnick (2016) reports on a survey by the Association of Clinical Research Organisations (ACRO) that there is high intensity to support IoT/IoMT due to the benefits talked about for precision medicine, but there must be security and privacy of the data. It's becoming clear why support is growing for blockchain and evidenced in surveys discussed in later sections of this research.

However, with this potential explosive increase in data also leads to more higher risks to security and privacy if not properly addressed. More and more data will be gathered and be a signature identity to the patient and create more unique biometrics.

2.7 Patient Centric Data Ownership

It has been mentioned that by sharing electronic health data across multiple organisations it can potentially save billions in cost, Monegain (2013). Research was undertaken by Premier Quest Alliance across 333 hospitals, that are members of the Alliance group, and analysis mentions by sharing the data, 92,000 lives were saved and with revenue savings of just over $9 billion over 4.5 years. Some key results of central-line associated blood stream infections reducing by 59 per cent and pressure ulcers by 64 per cent. If extrapolated nationwide, then 950,000 lives could be saved and savings of $93 billion. Saving lives is a key driver of healthcare services and blockchain can allow the discussion to be easier as it takes care of the more difficult questions on how to manage security and data sharing.

However, there are other reasons outside the saving lives and interoperability savings and revolves around healthcare data being a wealth of intelligence and by sharing this data it can improve the quality of services and innovations to make systems smarter and target precision medicine; Yue et al. (2016). With data currently scattered in silo mode in many different provider systems this makes the task of strategically looking at healthcare data in a smart way almost impossible. Many providers would be concerned on breaking the privacy parameters to patients if by sharing data in conventional ways. But equally and also worrying is that it is not reliable to leave responsibilities to Trusted Third Parties (TTP) where a single point of failure can be attacked, and data breached.

The innovative approach is to allow the patient to sit in the centre of all, have a concept of real-time monitoring of their health journey and essentially be in control. Having a patient centric driven model opens to other dimensions and use cases. Simply put, there would be a range and variety of stakeholders interested to mine the data available, with of course permission granted by patients. Research industry and other organisations will be keen to access this wealth of data to re-purpose to a number of initiatives that may be precision based medicine or unlock a number of new in-roads to solving diseases with smarter interventions. The data, if permissioned and released to industry, across millions of users can be anonymised and further protect patients since the core data is what is significant. Also, as mentioned

in the previous section, combining electronic medical data with smart data that has guaranteed accuracy (since it is recorded by sensors) again gives the healthcare industry huge confidence. Artificial Intelligence (AI) can also play a factor to help mine and analyse the data to better predict outcomes and correlations. There can be a Machine Learning aspect to 'train' these systems to intelligently predict and proactively offer intelligent insights for better decision making processes.

2.8 Other Blockchain Health Transformation Benefits

Whilst the above sections focus more on the blockchain tangible benefits of transformation in a sense of improving health, targeting precision medicine and patient outcomes, utilising the wealth of data intelligence etc., there are other benefits that can also equally play a strong factor for consideration and explained in the following.

2.8.1 Claims Adjudication

Currently there are many complex methods and processes to adjust and approve payment to claims made. There are estimations that 10% of healthcare costs are fraudulent. Das (2017) gives indication that in the US in 2016, Medicare fraud has caused $30 million in losses which could mostly be around non-performed services or excessive billing. By trusting the data shared, having easier data interchange process and automating the process and provide an immutable and auditable chain through smart contracts, can give a more transparent vision of the 'single version of the truth'. There should also be cost savings for applying more efficiency to the process in terms of facilitating payments more quickly and less communication required to do that. Many believe that there is scope to eliminate third parties such as clearing houses, third-part administrators, etc. There is a further interesting concept that ties into patient centric data and smart wearables and that is the possibility or real-time adjustments to premiums. If data from smart wearables is automated to smart contracts held on blockchain, then it may be possible to incentivise patients to better lifestyle as premiums can automatically re-adjust according to health risks and better well-being, etc., from data that is analysed. Presently if attempted in a conventional way then the method would be more static and require a lot of human intervention for applying a re-issued premium and how to audit it in a way that is trusted. If pursued through a blockchain method, then it will be more dynamic and responsive to the patient and its interactions and full audit trail given.

Blockchain can help manage better the high overhead healthcare administration costs that are inefficient with issues of duplication of requests. For example, some studies have been completed that indicate large amounts of budget are wasted in paperwork trails that are connected with insurance and billing claims and have

concerns over transparency on price; Jiwani et al. (2014). It makes sense that blockchain can help transform the processing side of healthcare administration as its would be configured to eliminate the duplicate processes and automate transactions and use smart contracts methodology to reconcile and audit all.

2.8.2 Drug Traceability and Issues in the Supply Chain

The issues around counterfeit drugs and its authenticity can have detrimental impacts for those connected along the supply chain to the patient. Deception and fraud lie amongst drug origin, expiry, compound mixtures that may be contaminated or wrong ingredients that impact effectiveness, wrong dosage, and the list can go on. There should be some secure method to manage all from raw materials to active pharmaceutical ingredient (API), to manufacturing, formulation, packaging and distribution. Where the supply chain is so sensitive to these external pressures there should be a positive momentum towards adopting blockchain as the layer to give the traceability, immutability, time-stamping through its smart contract process.

According to some research undertaken by the World Health Organisation there is evidence to suggest 10% of drugs worldwide are counterfeit and that dramatically increases in developing countries to 30%; Mettler (2016). Counterfeit drugs hold no boundaries and cross from supplement type to more treatment type drugs for disorders (e.g. cardio-vascular). They can have impure qualities, high or low dosages and if the patient relies on the active ingredients to work for health preservation then it becomes more high risk and dangerous to the patient. When blockchain is used, everything is time-stamped and recorded on the chain as to the production date, location and its product component origins. Ownership, in case of transfer to other parties is also transparent. Anything that is out of the chain is not verified and can be treated as forged until evidence is given as to the parameters set (or rules applied to smart contracts). The objectives to control and reduce counterfeit drugs could be achieved as well as potentially saving lives through controlling ineffective drugs that contaminate the supply chain.

Figure 2.8 explains how blockchain can be the mechanism to secure data from any tampering and help deter counterfeit drugs from entering the supply chain or the myriad of other issues discussed earlier in this section.

2.9 Is the Healthcare Industry Ready for Blockchain?

To gain confidence and global consensus (as well as prove the creditable research with evidential backed models that work) there should be blockchain pilots undertaken for analysis. In this section there are some leading examples of live deployment of blockchain within the healthcare industry. Each live deployment addresses

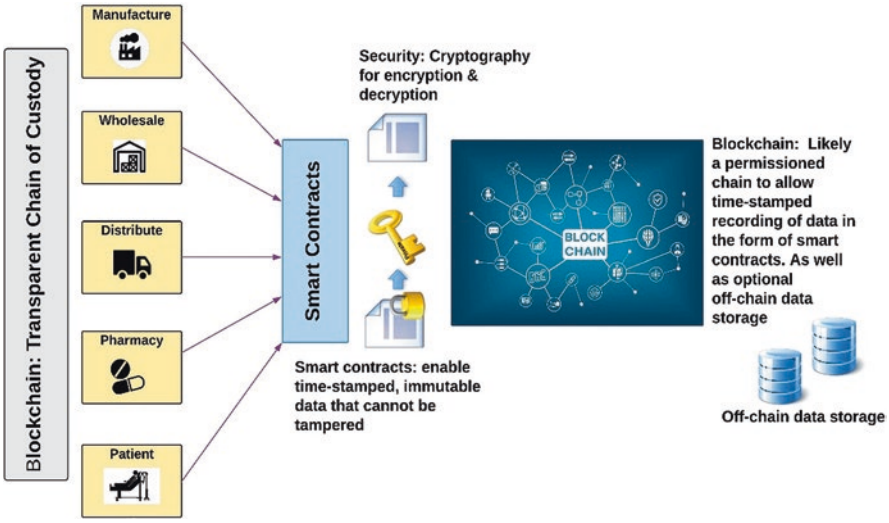

Fig. 2.8 Blockchain and the transparent chain of custody

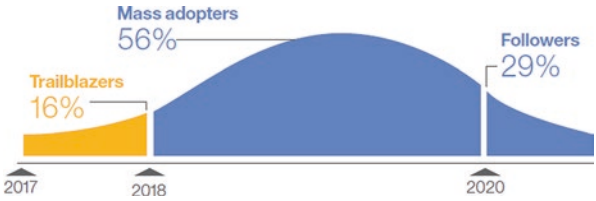

Fig. 2.9 Confidence with early adopters. (IBM Institute of Business value 2016)

issues such as interoperability, transparency, privacy, health data interchange, claims adjudication, drug traceability and supply chain integrity, to name a few.

Blockchain applications to the healthcare industry are version 3.0 which has evolved from blockchain version 1.0 for cryptocurrency and smart contracts deployment as version 2.0.

A recent survey (IBM Institute for Business Value 2016) of 200 healthcare executives (a mix of payers and providers across 16 countries) found that 16% were expecting to deploy a blockchain solution for healthcare soon. The survey holds a much higher percentage than other sectors of banking/finance and commerce which have been longer established in blockchain methodology than in healthcare. Figure 2.9 describes these early adopters as 'Trailblazers' and other Healthcare Institutions and a timeline of how the healthcare industry will react to adoption.

The IBM survey (Fig. 2.10) describes the friction areas around inaccessible information (the interoperability and security/privacy concerns on data) that both leading Trailblazers and other Healthcare Institutions mostly agree on. Also, they agree with the top three impact areas being **Clinical Trial Records**, **Medical Health Records** and **Regulatory Compliance**. The findings of the survey match well with the thrust of this research in the sense of although there is demand for open access

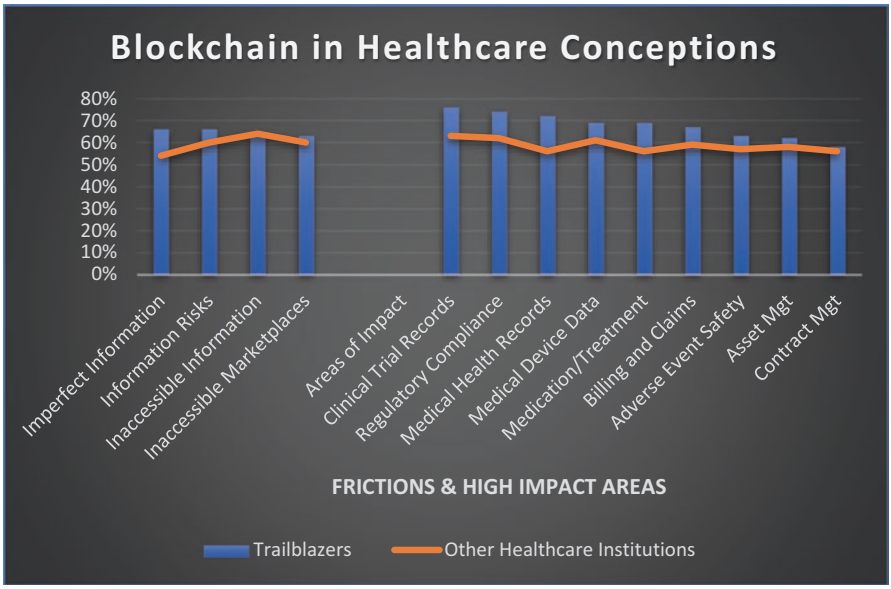

Fig. 2.10 Survey of 200 Healthcare executives; source a mix two data sets. (IBM Institute of Business Value 2016)

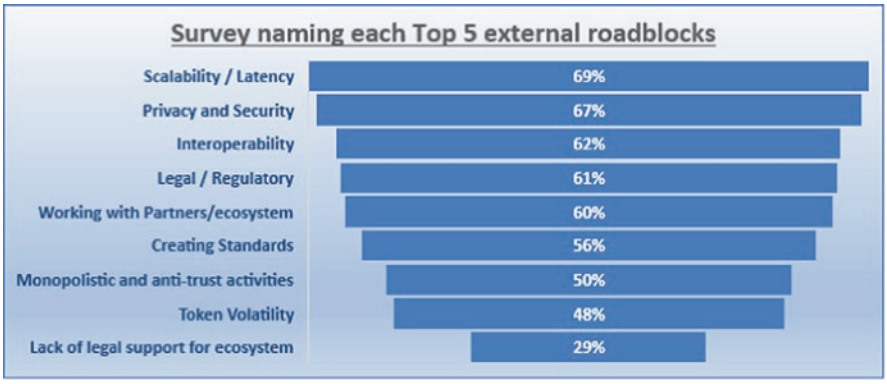

Fig. 2.11 Survey of 558 respondents proficient with blockchain in healthcare. (Cognizant 2017)

of trials data they agree that there is mistrust and data is hard to obtain/share where permissioned.

In Fig. 2.11, data was extracted to show a global survey of 558 respondents carried out by Cognizant (2017) and displays a similar outlook with regards to issues of privacy, security, interoperability and regulatory. The respondents were mostly considered proficient with blockchain and the survey asked respondents what they thought the top five external roadblocks would be.

The IBM Institute for Business Value (2016) survey has interesting points regarding *outcome switching* in clinical trials and survey comments match the research undertaken that data reported could be selective and should have greater transparency and sharing, which is explored further in Chap. 3. If the argument for withholding data was not to expose this data to competitors before public exposure, then blockchain would enable recording in real-time, be protected on blockchain through permissions and with the timestamp have an immutability so that it can't be denied.

To help validate the research and understand why interest in blockchain is growing, it is worth reviewing some blockchain healthcare initiatives that cover resolving a range of typical healthcare issues and explained as follows.

MedRec This was developed by MIT researchers (Azaria et al. 2016) and implemented in the Beth Israel Deaconess Medical Center (a teaching hospital of Harvard Medical School) to handle EHRs making use of existing blockchain technology and Ethereum smart contracts. Azaria et al. (2016) quote that it 'gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites'. This is one of the objectives, enforcing the rationale to use blockchain; to improve the interoperability, data sharing, transparency, and biomedical and outcomes research and benefit access to secure longitudinal research data, Angraal et al. (2017). The method is storing not the actual health record but signature of the record on the blockchain and this assures immutability and gives the patient control of access to the record and for those patients that may not want to control their data they may have the option to delegate these responsibilities; Halamka et al. (2017). Data is entered by the physician through the MedRec Provider App where stored data is accessed via a hashed link. The Ethereum blockchain controls the permissions and the patient has rights to download at any time as the blockchain authenticates valid privileges.

Guardtime In 2011, Estonia collaborated with a company called *Guardtime (*a Netherlands based company which conducts a blockchain architecture), to secure public and internal records and then after this initial success, in 2016, secured one million health records of Estonian citizens using its Keyless Signature Infrastructure (KSI); Mettler (2016). This innovation was a way to help solve the challenge to increase clinical health data exchange and interoperability and so improve transparency of the data. Estonia's embrace of blockchain technology has made it a country where 100% of its medical records are online in a secure and private method. The success of Estonia has given confidence to other regions such as in the UAE and a major healthcare provider there.

Gem Health Gem, a Californian based company partnered with Philips, created a blockchain healthcare ecosystem called the Gem Health Network and is a platform that sits on top of blockchain architecture and can easily deploy distributed applications, Ark Invest Research (2016). The aim was to connect all disparate arms of healthcare and with the patient at the centre as in control and have this community of patients, providers and industry all connected in a health data exchange, rather

than medical data in silo's, insurers claims on silo's, etc. As it's a permissioned blockchain it can control who can access sensitive information and ensures anonymity (patient information can't be linked to a patient in an event of a data breach).

Healthbank Based in Switzerland, the *healthbank* mantra is "my data, my choice, my *healthbank*", Nichol (2016). The data control is left to the user (hence the quote explains the meaning) and can even chose to provide data for medical research and perhaps receive financial compensation and if the patient data is of significant value they may be rewarded at a higher than normal rate, Mettler (2016). In this way *healthbank* becomes a patient driven system and blockchain is being further investigated to ensure fast, secure and authenticated access to patient data. This is a good example of ways to look at improving transparency and security in the clinical research world.

Pokitdok An API platform-as-a-service allowing users to interact with over 700 trading partners and use identity management to validate the partner transactions involved. This can help facilitate what was once data held in silos and now having seamless interaction. For example, near instant billing and insurance claim resolution, Engelhardt (2017).

Patientory A start-up that believed there was a need for more collaboration between providers and patients to allow more connectivity and transmit data securely using blockchain technology. They also developed a mobile healthcare app to help patients keep a track on their medical history, bills, pharmacy medications, insurance and so on, Slabodkin (2017). Interestingly patients can also connect with other patients for similar health problems.

Modum Founded in 2016 and designed to help improve the pharmaceutical for supply chain monitoring. Traceability and compliance are difficult in current scenarios and blockchain helps cut down on the paper trail and provide a more tamper proof system that is auditable along all its journey. This is particularly specific in the pharmaceutical industry where in some regulation compliance it is essential that deviations are reported in temperature, light conditions, humidity, etc., as IoT sensors monitor the temperature of the products and sensor data and is transferred to the blockchain. A smart contract is initiated thereafter (this is the integrity and immutability the system offers) and the data recordings are compared what is measured against the compliance requirement. Should a deviation occur then a notification is released to the parties required to know, Schumacher (2017).

iSolve The Advanced Digital Ledger Technology is a solution by iSolve that manages the life cycle of drug development and drug supply chain in the biopharma and healthcare industry by using blockchain as the mechanism to track, audit and record all logistical movement of medications. Data sharing and transparency are key components to the system. There is a need to have meticulous tracking due to counterfeit and fraudulent drugs and medications. This issue is highlighted more in regions

where regulation and legal frameworks are not mature or right controls and monitoring. Blockchain can handle the life cycle from development to distribution so even something simple like expiry dates can be driven with accuracy and negate the chances of fraudulent relabelling of changing of dates; Engelhardt (2017). iSolve also manages the acquisition of IP assets, can raise funding and advance drug development through Smart Market where information is held in a secure method and is trackable, immutable and visible as a marketplace to investors and service providers.

Medicalchain A distributed ledger that allows permissioned based blockchain to securely store health and patient records and the user to give permissions to healthcare professionals (these could be doctors, pharmacists, hospitals and laboratories) for access to their personal medical data. The transactions are recorded/audited in a transparent manner, but privacy of the patient is of key importance. This takes care of interoperability issues and the scenario of fragmented healthcare services. If information could be more integrated then it may help lessen medical errors as some research undertaken by McMains (2016) at the John Hopkins Hospital in the US concludes that medical errors are the third leading reason for deaths (in the US). This may be due to the uncoordinated healthcare approach of silo data.

BurstIQ Blockchain enabled for securely handling person-centric data, as an authenticated and permissioned interchange, connecting any data from any source. The model allows researchers, businesses and individuals to connect and share data. Individuals can decide if and when to share, sell or even donate their data; accessed through their HealthWallet. This could cover electronic medical data and other such as diagnostic, behavioural, fitness, pharmaceutical, smart data, etc.

2.10 Conclusions

The healthcare industry is no stranger to undergoing transformation of its paper and manual processes to more digital and electronic methods and associated data workflows. As technology has advanced, so too has the delivery of more precision based medicine and the Internet of Medical Things (IoMT) has opened up an abundance of many smart sensors and devices culminating in large collation of data and behaviours that can help determine better outcomes at point of care. But although beneficial with the digitalisation of medical records these are still stored in many disparate silos and healthcare is now suffering the most cyber-attacks resulting in significant data breach losses and identity theft than any other sector. Blockchain presents itself to be a fit for purpose solution to a wide range of legacy issues that have dominated the healthcare industry. These legacy issues have tended to provide the patient weaker perspectives and offer risks that may have wide and far reaching consequences. As medical science evolves, then so too must the mechanism and tools that support how all the data is protected and handled.

References

Angraal et al (2017) Blockchain technology: applications in healthcare. Circ: Cardiovasc Qual Outcomes 1–4. Available at: https://doi.org/10.1161/CIRCOUTCOMES.117.003800. Accessed 20 Oct 2018

Ark Invest Research (2016) How blockchain can enhance EHR operability. Available at: http://research.ark-invest.com/blockchain-and-healthcare. Accessed 20 Oct 2018

Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: using blockchain for medical data access and permission management. In: 2nd International conference on Open and Big Data (OBD), Vienna, pp 25–30. Available at: https://doi.org/10.1109/OBD.2016.11. Accessed 20 Oct 2018

Bresnick J (2016) How will internet of things devices impact precision medicine. HealthIT Analytics. [Online]. Available at: https://healthitanalytics.com/news/how-will-internet-of-things-devices-impact-precision-medicine. Accessed 20 Oct 2018

Cognizant (2017) Healthcare: blockchain's curative potential for healthcare efficiency and quality. [Online]. Available at: https://www.cognizant.com/whitepapers/healthcare-blockchains-curative-potential-for-healthcare-efficiency-and-quality-codex2995.pdf. Accessed 20 Oct 2018

Das R (2017) Does blockchain have a place in healthcare? Forbes. [Online]. Available at: https://www.forbes.com/sites/reenitadas/2017/05/08/does-blockchain-have-a-place-in-healthcare/#42a2eeba1c31. Accessed 20 Oct 2018

Dubovistskaya A et al. (2017) Secure and trustable electronic medical records sharing using blockchain. In: AMIA 2017 annual symposium proceedings. [Online]. Available at: https://arxiv.org/abs/1709.06528. Accessed 21 April 2018

Engelhardt M (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innova Manage Rev 7(10):22–34. Available at: https://doi.org/10.22215/timreview/1111. Accessed 20 Oct 2018

Halamka J et al (2017) The potential for blockchain to transform electronic health records. [Online] Available at: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records. Accessed 20 Oct 2018

IBM Institute for Business Value. (2016) Healthcare rallies for blockchains: keeping patients at the center. [Online]. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03790USEN. Accessed 31 May 2018

Jiwani A, et al. (2014) Billing and insurance-related administrative costs in United States' health care: synthesis of micro-costing evidence. BMC Health Serv Res 14: 556. [Online]. Available at:https://doi.org/10.1186/s12913-014-0556-7. Accessed 20 Oct 2014

Labchain (2018.) Available at: https://www.labchain.nl/. Accessed 20 Oct 2018

Liang X et al. (2017) Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: IEEE 28th annual international symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, pp 1–5. Available at: https://doi.org/10.1109/PIMRC.2017.8292361. Accessed 20 Oct 2018

Linn L, Koo M (2016) Blockchain for health data and its potential use in health IT and health care related research. [Online]. Available at: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf. Accessed 20 Oct 2018

McMains V (2016) John Hopkins study suggests medical errors are third-leading cause of death in U.S. John Hopkins University. [Online]. Available at: https://hub.jhu.edu/2016/05/03/medical-errors-third-leading-cause-of-death/. Accessed 20 Oct 2018

Mettler M (2016) Blockchain technology in healthcare: the revolution starts here. In: IEEE 18th international conference on e-health networking, applications and services (Healthcom), Munich, pp 1–3. Available at: https://doi.org/10.1109/HealthCom.2016.7749510. Accessed 20 Oct 2018

Monegain B (2013) Data-sharing initiative reduces deaths. Healthcare IT News. Available at: https://www.healthcareitnews.com/news/data-sharing-initiative-reduces-deaths. Accessed 20 Oct 2018

Nichol, P. (2016) Blockchain applications for healthcare. [Online] Available at: http://www.cio.com/article/3042603/innovation/blockchain-applications-for-healthcare.html. Accessed 20 Oct 2018

ONC (2015) Connecting health and care for the nation: a shared nationwide interoperability roadmap. [Online]. Available at: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf. Accessed 20 Oct 2018

ONC (2016) Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008–2015. [Online]. Available at: https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php. Accessed 22 Oct 2018

Rifi Net al (2017) Towards using blockchain technology for eHealth data access management. In Fourth International Conference on Advances in Biomedical Engineering (ICABME), Beirut, pp. 1–4. Available at: https://doi.org/10.1109/ICABME.2017.8167555. Accessed 6 May 2018

Schumacher A (2017) Blockchain & Healthcare. 2017 Strategy Guide for the Pharmaceutical Industry, Insurers & Healthcare Providers. [Online]. Available at: https://www.researchgate.net/publication/317936859_Blockchain_Healthcare_-_2017_Strategy_Guide. Accessed 20 Oct 2018

Slabodkin G (2017) Blockchain remains a work in progress for use in healthcare. Health Data Manag. [Online]. Available at: 2017. ProQuest, https://search.proquest.com/docview/1914536464?accountid=12860. Accessed 20 Oct 2018

Yue X et al (2016) Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 40(10):1–8. [Online]. Available at: https://doi.org/10.1007/s10916-016-0574-6. Accessed 20 Oct 2018

Zevala C (2017) How IoT is improving the accuracy of clinical research. IoT Evolution. [Online]. Available at: http://www.iotevolutionworld.com/m2m/articles/431211-how-iot-improving-accuracy-clinical-research.htm. Accessed 20 Oct 2018