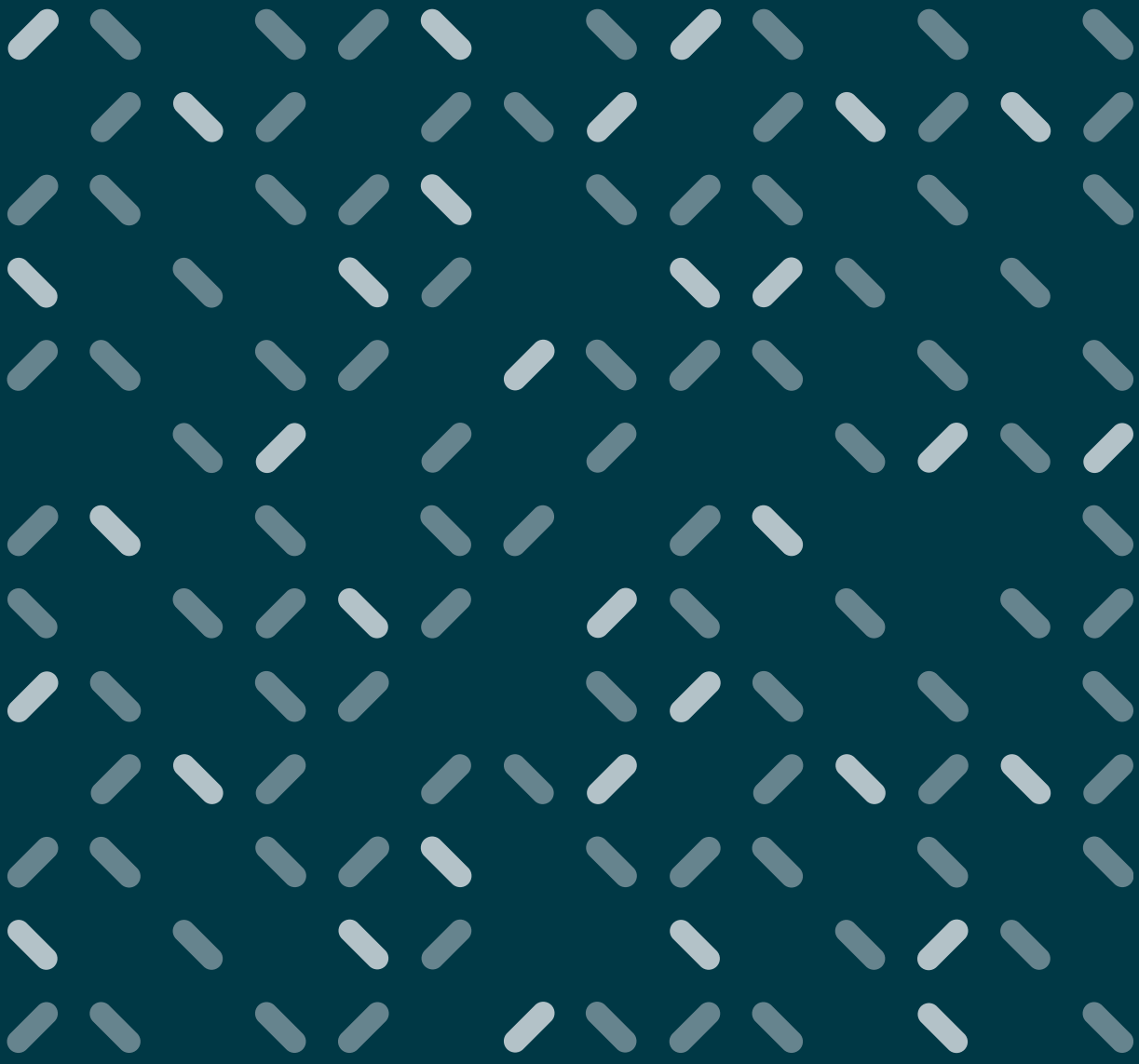
Norwegian Centre for
E-health Research

PROJECT REPORT

Blockchain and Digital Health

A scoping review

Chomutare T, Yitbarek Yigzaw K, Linstad L, Nordsletta AT.



Blockchain and Digital Health

A scoping review

Report number
09-2017

Project manager
Per Atle Bakkevoll

Authors
Taridzo Chomutare, Kassaye Yitbarek Yigzaw, Line Linstad, Anne Torill Nordsletta

ISBN
978-82-8242-078-5

Date
22.09.2017

Pages
14

Keywords
Blockchain, cryptocurrency, DLT, eHealth, EHR

Summary
As with any new technology, the hype may not always have sufficient substance to make the transformation to real value. Blockchain is the technology underlying bitcoin, and is gaining considerable interest from the public sector, big corporations and leading research schools around the world. To date, general public understanding of blockchain is limited and the implications for digital health are still poorly understood. The technology promises to improve security and privacy in the era of digital health, but faces a number of technological, legal and organisational challenges. This report examines the discussion in the scientific community as well as in commerce and industry; to provide a balanced scope of the narrative regarding the implications of blockchain in healthcare.

Publisher
Norwegian Centre for E-health
PO Box 35
9038 Tromsø
E-mail: mail@ehealthresearch.no
Web: www.ehealthresearch.no

Table of Contents

1 Introduction 4
1.1 Executive Summary 4
1.2 About the report 5

2 Methods 5
2.1 Scoping review of the literature 5
2.2 Grey literature 5

3 Primer on blockchain 6
3.1 Brief history of adoption 6
3.2 Why now? 6
3.3 How Blockchain works 7

4 Literature on blockchain in healthcare 8
4.1 Summary of included articles 8
4.2 Themes emerging from the literature 9
4.3 Peer-reviewed idea white papers 10
4.4 Examples from industry, commerce and research 11
4.5 National implementations and government initiatives 11
4.6 What are the knowledge gaps and challenges? 12

5 Conclusion 12

6 References 13

List of tables and figures

Figure 1. Most common transaction type. Source:O'reilly [1] 7

Table 1: Themes emerging from the reports in the literature 8

Glossary of terms

Address: Used in cryptocurrencies, an address is an alphanumeric token used to represent the destination for a payment.

Blockchain/Ledger: Is a record (chain) of transactions that can only be added to and is tamper-proof, and is shared and distributed in the network.

Consensus: Is a de-centralised protocol for network actors to verify transactions and agree on the contents of the ledger.

Cryptocurrency: Is a form of digital currency, using cryptography to self-regulate, without the need for a central bank or authority.

Mining: Is the process where network participants verify transactions and add them to the ledger. In permission-less ledgers, anyone in the network can be a miner, and miners are free to come and go. In permissioned ledgers, the miners are known in advance.

Off-chain data: This refers to the use of references that point to data that resides outside the blockchain. This is part of proposed solution for using blockchain with patient data, but it should be noted that blockchain can secure data stored on the chain and cannot guarantee the state of data stored elsewhere.

Participant/party/node/peer: This refers to network clients or computer programs that have access to the ledger and can potentially add transactions.

Permissioned ledger: This is where network participants have advance permission to verify transactions in a limited consensus process. These are proposed as private ledger solutions for corporations or other public and private institutions that are trusted.

Permission-less ledger: This is the original framework designed for an open network where any network node can participate in consensus building, without the need for any trusted third party.

Smart contracts: These are specified rules enforced automatically by the network actors, and are encoded in a computer program. For example, smart contracts for executing specific transactions when certain criteria are met. These can be contrasted to legal language that can be difficult to interpret and is also susceptible to breach of contract.

Transactions: Are the activities of transferring ownership, for example, using a Bitcoin address to transfer bitcoin. In healthcare, it is proposed this could be adding data about a test, diagnosis or lab result for a patient.

1 Introduction

1.1 Executive Summary

Blockchain, a distributed ledger technology (DLT), underlies decentralized cryptocurrencies like bitcoin [2] and is the world's leading software platform for digital assets. It is gaining considerable interest from the public sector, big corporations like IBM and leading research schools [3]. The future impact of blockchain is unknowable, but critical analysis and research may help us keep abreast of the potential benefits and harms, thus also avoiding unproductive scepticism that mars the history of many great inventions. One example often cited is the Western Union internal memo (1876) - "This *'telephone'* has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us."

Blockchain relies on redundant copies of a public ledger of transactions distributed over several nodes on the network. Cryptography is used to secure blockchain, and the record of transactions is immutable, meaning it is tamper-proof. This immutability property, together with redundancy, make it possible to prevent double-spending of resources; qualities that made blockchain a protocol of choice for cryptocurrencies such as bitcoin.

Recent narrative suggests blockchain has the potential to influence developments in sectors other than financial technology; from healthcare to unlikely areas such as conservation and biodiversity [4], to outlandish claims of alleviating world poverty[1]. The technology has been touted as a security and privacy panacea for connected health ecosystems that are already experiencing increasing volume of sensitive personal data. So far, however, we know little about the organisational, legal or technical implications of large scale blockchain implementation [5]. Scientific research is still in its infancy and there exists only a few large-scale case studies from which to learn.

This report provides a general scope of the discussion in the research community as well as in industry and commerce. The general themes that seem to emerge from the scientific community regarding blockchain in healthcare include (i) security and privacy, (ii) research and public health, (iii) Internet of things and personal health sensor data, (iv) electronic health records (EHR), personal health records (PHR) and interoperability, and (v) the illicit activities on the web. Blockchain appears to be an obvious path for more secure connected health in the future. However, there still remain a number of technical, legal and organisational challenges that require consideration. Technically, there are still questions regarding scalability, cryptographic techniques, privacy and general user-friendliness, to name a few. In terms of organization and legislation, blockchain is originally designed for an open network without any governance model; therefore the role of government agencies in providing consumer protection and legal recourse is less clear.

Today, government agencies and health institutions are important intermediaries that have centralised responsibility and oversight on national healthcare systems, for example Norway's strategic efforts towards "one citizen, one journal"[2]. If in the future some of the technical and organisational challenges become fully or partially clarified, adoption of blockchain in new and untested healthcare settings may gain more attention. The evidence so far appears insufficient to make a solid case for or against blockchain; therefore further research is required before the implications for healthcare can be more clearly understood.

---

[1] https://www.forbes.com/sites/nikolaikuznetsov/2017/07/24/how-emerging-markets-and-blockchain-can-bring-an-end-to-poverty/#50f2becf4a0c

[2] https://www.regjeringen.no/no/dokumenter/meld-st-9-20122013/id708609/

1.2 About the report

As with any new technology, the hype may not always have sufficient substance to make the transformation to real value. The objectives of this report are two-fold; to provide: (i) a high level introduction to the adoption of blockchain and cryptocurrencies, and (ii) a scoping review of the literature related to blockchain in digital health. This report does not formally evaluate potential sources of bias, such as rigor of research method in the published articles. However, it is hoped a critical analysis will give readers a balanced scope of the narrative.

2 Methods

Initially, two workshops were held on the topic, one on 14.11.2016 and the other on 21.06.2017 at the Oslo Science Park. The workshops were organised by Alpha Venturi AS and Oslo Cancer Cluster, and had representatives from both government and industry in Norway, Finland, United Kingdom and Estonia. Represented institutions and companies included The Norwegian Directorate of eHealth, Oslo Cancer Cluster, Oslo Medtech (now Norway Health Tech), University of Oulu, Nordic Innovation, Teknologirådet, Guardtime, Kreftregisteret, Alpha Venturi AS, Amgen, Digi.me, Nye Metoder and Norwegian Centre for E-Health Research. In addition, a short seminar was held at Norwegian Centre for E-Health Research in April of 2017 to initiate both ideas for scientific inquiry and general awareness about the topic. Blockchain was also discussed at the EHiN 2016 conference.

Partly as a result of these brainstorming initiatives, a scoping review seemed like an appropriate methodological approach for constructing this report. The method was used to extract thematic areas from peer-reviewed publications in order to assess the general breadth of the discussion. In addition, grey literature was used to find articles that are not available in standard research databases, and these could be blogs or reports from experts and corporate or government websites.

2.1 Scoping review of the literature

Databases of scientific publications in both medicine (PubMed, EMBASE, PsycINFO) and computer sciences and engineering (IEEE, ACM, DBLP) were searched for relevant articles. The search terms used were “blockchain”, “bitcoin”, “DLT”, “cryptocurrency”, with a conjunction on “health*”. We selected any scientific study that included both blockchain and healthcare in their discussion, even if these topics were not the main purpose of the publications. The search included text of scientific articles, and not just the title and abstract. In terms of data extraction, thematic areas were identified in each source that dealt with both blockchain and healthcare applications. No initial template was used for extracting these themes. In addition, the dates and geographical location of the publishing institution was also recorded.

2.2 Grey literature

There is a lot of information about the topic on the Internet and much of it is not published in scientific journals. It is therefore necessary to uncover information that may not have a basis in scholarly research, including implementations by commerce and industry. Important corporate developments often precede publication in academic journals.

Another source that informs this report is The Office of the National Coordinator (ONC) for Health Information Technology in USA. They invited idea papers in a challenge on blockchain in healthcare on their website (www.healthit.gov) in August 2016. They received about seventy submissions, and they short-listed fifteen for prizes. This report reviews the short-listed papers to document these less developed ideas, vision statements and early reporting of research activities.

3 Primer on blockchain

3.1 Brief history of adoption

The most popular DLT is probably Blockchain, the underlying technology behind bitcoin. The true identity of the inventor, the person or persons or institution is unknown, except with a Japanese pseudonym Satoshi Nakamoto, the person who submitted the initial 2009 whitepaper [6]. The market capitalization of bitcoin in September 2015 was about NOK 30 billion (USD 3.4 billion) and according to www.coinmarketcap.com as of 01 September 2017, the market capitalization has increased to over NOK 500 billion (>USD70 billion), albeit with high volatility. Even though some experts have speculated this could be a huge pricing bubble, the currency seems to continue to gain legitimacy as world governments embrace cryptocurrencies in different ways. The prevailing environment has encouraged the incubation of a plethora of cryptocurrencies such as Litecoin, Ripple and Ethereum.

Less than 5 years ago, many governments would not sanction cryptocurrency dealings of any form. Recently however, the trend is changing, with governments such as Russia even reversing their previous adversarial stance against bitcoin, according to a recent article by www.bitcoin.com . As of April 2017, Japan recognizes bitcoin and Ethereum as legal means of payment[3]. While the official status of bitcoin is still either unclear or unregulated in many countries, trading in the cryptocurrency is legal in most countries worldwide. In a recent report by Reuters, one of the world's biggest bitcoin exchanges (BTCC) based in China decided to shutdown, citing regulatory tightening.

In a bid to increase the appeal of bitcoin and its wider adoption through convenience, new bitcoin ATMs were introduced in Austin, Texas in 2014, and the number has grown to more than 1500 ATMs worldwide as of 01 September 2017, according to www.coinatmradar.com. Most (>70%) are in USA and Canada, and Europe (>20%), while the rest of the world hold the remaining. Start-ups are now raising instant funds in cryptocurrency through Initial Coin Offering (ICO), and this market has surpassed a billion US dollars (see www.coinschedule.com for live token sales).

The relevance of today's banking system to cryptocurrencies is uncertain. In 2014, R3CEV LLC formed a consortium of seventy of the world's largest banks to explore blockchain. However, some of the banks have begun exiting the consortium. For example, the Bank of Canada cited *"fundamental inconsistencies"* with centralized systems, after testing blockchain for a year[4]. The Canadian case demonstrates how the technology is not suited for centralised infrastructures such as banks, since the initial philosophy of blockchain avoids any centralised broker. Perhaps blockchain requires a new way of thinking; something that disrupts current financial systems, potentially making them obsolete.

3.2 Why now?

This report comes at a time when cryptocurrencies seem unstoppable, with more and more businesses accepting digital currencies as payment, and governments removing prior restrictions. There is general euphoria and excitement around application of blockchain to areas other than finance. While such excitement often generates innovative new applications, it can also remain just hype. Proponents put blockchain in the same class as artificial intelligence (AI), machine learning, natural language processing (NLP) and internet of things (IoT), in terms of important emerging technologies. This reports attempts to organise the narrative and assess potential applications in healthcare.

---

[3] http://spectrum.ieee.org/tech-talk/computing/it/japan-takes-lead-in-legitimizing-digital-currencies

[4] http://www.reuters.com/article/canada-cenbank-blockchain/bank-of-canada-says-wont-use-blockchain-for-interbank-payment-system-idUSL1N1IP2CK

3.3 How Blockchain works

Unlike traditional databases that are stored and maintained on private and centralised servers, a blockchain is distributed and maintained by hundreds, thousands or even millions of computers all over the world. Bitcoin is based on a peer-to-peer network, meaning transactions can occur between two or more parties, without the need for an intermediary such as a banker or government agent. Blockchain is a public ledger of transactions where all nodes on the network can view the ledger, and the ledger is not controlled by any one node. Once a transaction is approved, it becomes part of the blockchain ledger, and the ledger cannot be tampered with.

Some nodes in the network, called "miners", get rewarded with bitcoins for adding blocks to the blockchain. This reward mechanism enforces miners to behave as the majority. That means in a network with 51% honest miners, a miner should remain honest to be able earn the reward. Since there are no trusted third parties or intermediaries such as banks, miners collaborate to form a consensus about transactions. Theoretically, any computer can be a miner, but in practice, specialised hardware is recommended.

In summary, the distributed consensus (Bitcoin protocol), public ledger, mining and block transaction verification systems are the four key innovations on which the cryptocurrency is founded [1]. Transacting bitcoin is merely an exchange of data, whose log is appended to previous transactions, forming a ledger of connected transactions, hence the 'chain' analogy. Recent implementations such as Ethereum support multiple data types and smart contracts. Smart contracts are rule-based algorithms for performing actions when certain criteria are met. Figure 1 is a simple illustration of the most common type of transaction.

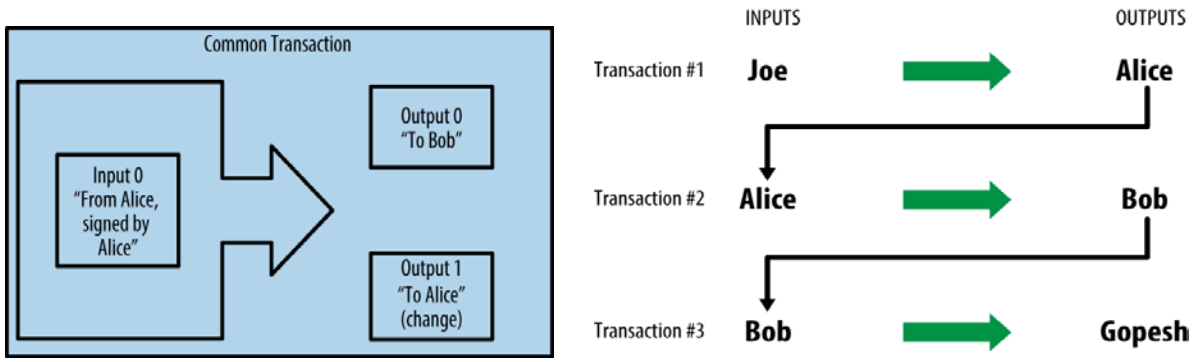


Figure 1. Most common transaction type. Source:O'reilly [1]

From Figure 1, the most common transaction example given in [1], the transaction has one input and two outputs. Alice sends a payment to Bob's address, and sends the difference or "change" to an additional address that she controls. In the example, Alice's transaction will be mined, approved and become part of the block. Through the ledger, anyone can inspect how Alice earlier on had received payment from Joe (Transaction#1), which she used to pay Bob (Transaction#2). Even though the record of transactions is public, there are techniques used to make it difficult to trace transactions to anyone. It is recommended that addresses be used only once to improve privacy. This is not completely bullet proof, so techniques such as coin mixing have been developed to increase users' anonymity. On the other hand, development of de-anonymization algorithms for finding links between addresses has become a research topic, possibly important for auditing, law enforcement and marketing. For further reading on bitcoin, cryptocurrencies and the blockchain:

A) Bitcoin & Cryptocurrency Technologies: A Comprehensive Introduction; Princeton University Press [7]
B) Mastering Bitcoin; O'Reilly [1]

4 Literature on blockchain in healthcare

4.1 Summary of included articles

In total, 22 published articles met the selection criteria and were included in the analysis (see Table 1). From the medical literature 36 hits were returned, but only 12 were relevant to both blockchain and healthcare. Technical databases returned 14 studies, and after removing duplicates, 10 met the selection criteria. The major themes emerging from these studies include (i) security and privacy, (ii) research and public health, (iii) Internet of things and personal health sensor data, (iv) electronic health records (EHR), personal health records (PHR) and interoperability, and (v) the illicit activities on the web.

Most of the included articles (n=13/22) were original scientific studies conducted in 2017, while the rest were editorials, commentaries, short communications and case studies. Some of the original studies were methods articles, demonstrating methods for implementing blockchain in the specific use-cases using a fully or semi-fully functional prototype. While we did not formally assess the scientific quality of the articles, methodological approaches seemed generally weak. One study by Irving and Holden [8] was eventually retracted from the PubMed index, after the authors received criticism for seriously flawed methodology.

One criticism that can be levelled against much of the literature is that studies only demonstrated the technical properties of blockchain that we already expect, and only a few dealt with practical challenges. For example, can patients handle data ownership and private key management, can legacy systems easily integrate with blockchain, what are the implications on organisation, can vendor support be mobilised?

Table 1: Themes emerging from the reports in the literature

Reference	Date	Location	Themes	
Zhao et al. [9]	May 2017	China	Security; private key management, access control	Data access
Benchoufi et al. [10]	Jun 2017	France	Research; data transparency in clinical trials	
Nugent et al. [11]	Sep 2016	UK	Research; data transparency in clinical trials	
Skiba DJ [12]	Jul 2017	USA	Research; audit of medical education	
Mettler M [13]	Oct 2016	Switzerland	Research; public health, drug provenance	
McKernan KJ [14]	Oct 2016	USA	Research; open DNA sequence database	
Hoy MB [15]	Jun 2017	USA	Research; libraries and medicine	
Salahuddin et al. [16]	Jun 2017	Canada	Internet of things and sensor data	Operations on data
Zhang et al. [17]	Nov 2016	China	Internet of things and sensor data	
Hashemi et al. [18]	Apr 2016	USA	Internet of things and sensor data	
Smith et al. [19]	Apr 2017	USA	EHR; security	
Roerhs et al. [20]	Jun 2017	Brazil	EHR; Interoperability; PHR	
Zhang et al. [21]	May 2017	USA	EHR; interoperability	
Yue et al. [22]	Sep 2016	China	EHR; interoperability	
Ichikawa et al. [23]	Jun 2017	Japan	EHR; immutable record	
Xia et al. [24]	Jun 2017	China	EHR; data sharing and access	
Azaria et al. [25]	Aug 2016	USA	EHR; data sharing and access	
Barratt et al. [26]	Aug 2016	Australia	Darknet; illegal drug trading	
Van Hout et al. [27]	Feb 2014	Ireland	Darknet; illegal drug trading	
Masoni et al. [28]	Oct 2016	Italy	Darknet; illegal and counterfeit drug trading	
Portnoff et al. [29]	Jul 2017	USA	Darknet; human trafficking and prostitution	
Mackey et al. [30]	Mar 2017	USA	Darknet; drug supply chain provenance	

4.2 Themes emerging from the literature

There seem to be generally two types of applications of blockchain to healthcare: (i) applications in distributed access control, consent and smart contracts, and (ii) applications in transacting on patient data in journals (EHR). The former class deals with themes related to access control for viewing or analysing patient histories or accessing data for research. The latter class deals with transactions like adding tests or diagnosis from the point of care, and updating references on the blockchain.

Privacy and security emerged as the overall problem that blockchain can solve in healthcare. Therefore, most of the identified themes have undertones of security and privacy. Only one study actually dealt with the issue of managing private keys [9]. Blockchain is based on digital signatures where a patient signs a transaction using his/her private key and anybody can verify whether the transaction was signed by a private key that belongs to the patient. The validation is performed using the user's public key, which is publicly available. If the private key is deleted or lost, proof of ownership is also lost and not recoverable, and whoever has the private key will be able to access and use the digital assets. Of course, when used properly, private keys provide a mechanism for securing health data.

Research and public health is another theme emerging from the search, where blockchain could be used to improve the conduct of clinical trials; from identifying relevant cohorts, obtaining their consent to defining the research protocol, regulatory compliance and sharing data obtained in the studies. Using blockchain in clinical trial registration for instance, anyone can have a copy of a predefined research protocol that cannot be altered later or omitted when reporting, thus reducing the impact of major sources of bias when reporting clinical trials, e.g. reporting bias and altering outcome measures. Nugent et al. [31] actually demonstrated how a clinical trial can be documented securely, even though the study focused more on the technical details rather than the organisational implications.

Internet of things (IoT) and ubiquitous health sensor data is a theme discussed by three studies. Two [16, 17] of the three studies described their prototypes, showing how sensor data generated by patients could be managed with blockchain. Patient-generated data (and sensor data) can become part of the immutable clinical record that is also available to healthcare providers. Much of the described work is technical, namely, the communication protocols and how data is moved and transacted on the blockchain.

Interoperability of EHRs is another important theme discussed in the literature. Blockchain promises a resource for uniformly accessing and updating patient data that are situated at different healthcare institutions, including patient-generated data. However, the argument for interoperability appears not fully developed since blockchain does not intrinsically solve the basic semantic interoperability problems associated with integrating different EHRs. It takes a great deal of effort to have systems agree on communication standards, but perhaps blockchain could be a catalyst for such developments if other benefits of blockchain are perceived as attractive enough.

Illicit activities is the final theme discussed in the literature. Anonymity of surfing hidden websites using custom privacy software, coupled with anonymous payment systems seem to create an ideal environment for crime to thrive. Human trafficking and prostitution on the web with bitcoin [29] has been reported, but by far the leading theme pertains to illegal and counterfeit drugs sold on the so-called darknet, such as the now defunct Silk Road[5]. Conversely, blockchain can also be used in positive ways, such as in drug provenance, that is, in the audit of the drug supply chain to prevent counterfeit drugs. Securing the drug supply chain is possibly one of the most promising use-cases, since blockchain-like systems are already in use today.

[5] https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

4.3 Peer-reviewed idea white papers

The short-listed white papers included submissions from IBM, Deloitte Consulting LLP, MIT, Accenture plc and Mayo Clinic, and are listed on www.healthit.gov. Much of the discussion in these papers is based on authors' vision, but no implementation studies or pilots are reported to have been carried out. Most of the idea papers are not based on scientific research, and in many places citing personal blogs and other less authoritative Internet sources. However, the report by Ekblaw et al. [25] from MIT reported work on MedRec, an actual prototype that uses blockchain, albeit not yet evaluated in a pilot study. Drew Ivan's white paper provided a more sober discussion of the practical implications of introducing blockchain to EHR systems; the risks of moving health data to unproven platforms, the organisational implications, costs and incentives required to persuade vendors to move to blockchain.

One limitation of the discussion in the white papers is that it is written for a specific public agency in USA, and some of the assumptions are not true for Norway. For instance, some of the papers dealt with the problem of trusted sources of identity data; Master Patient Index (MPI), for identifying patients across systems. In Norway, personal identity numbers are trusted identities across many important digital services in banking and healthcare. Another irrelevant area is the insurance claims. The US environment has multiple health insurance companies, means-tested federal health insurance schemes and private health care institutions with systems that are not integrated. This contrasts with much of Europe, including Norway, which has national health insurance schemes.

The paper from IBM discussed trust and verified identity as important facets of commerce, and how intermediaries can be inefficient. Shrier et al.[6] from MIT reported on OPAL/Enigma, a peer-to-peer platform that enables secure access to health data through using secret sharing and multi-party computation. They proposed blockchain using permissioned ledger to ensure parties who query the distributed databases have the right to do so, and that a permanent audit trail is available for inspection. Peterson et al.[7] from Mayo Clinic discussed information exchange networks, and the blockchain infrastructures that potentially increase security in patient data exchange across institutions, as well as consideration of semantic interoperability using open standards like HL7 Fast Healthcare Interoperability Resources (FHIR)[8].

One key take-away from the paper from Deloitte[9] LLP was the four item checklist that can be useful when contemplating using blockchain as a solution for transacting on electronic health data. The first item requires that there must be multiple parties that transact on the same resource. The question is whether the number of participants is large enough, and independent enough to justify the blockchain solution. The second item is that all the parties need to trust that the contents of transactions are valid. It is important for the healthcare service to trust data about the patient, including data generated at other institutions and patient-generated data from sensors.

The third item is the assumption that trusted third parties are inefficient. This could mean the patient gets more control of their own data, and share as they see fit, rather than trusting a hospital to control access. While this may initially sound appealing, there is not enough research on whether patients prefer to have control and whether they are able to do so securely. The fourth and final item requires that there is a strong need for security. Indeed, some have argued health data needs more security than banks. However, Deloitte's framework or checklist seems most suitable only when considering implementing a distributed blockchain-based health journal, and is less relevant for other possible use-cases.

---

[6] https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

[7] https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf

[8] www.hl7.org/fhir

[9] https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html

4.4 Examples from industry, commerce and research

There are several examples from large corporations such as IBM to small start-ups, such as Pillar Lab, a Norwegian start-up in blockchain-related technologies. IBM is a co-founding member of the open source blockchain project Hyperledger[10]. They further developed the Hyperledger platform, and created toolkits for rapid prototyping of blockchain applications. They recently announced a multi-million dollar project "Watson IoT Private Blockchain" in Germany[11], a private blockchain initiative.

Another corporate giant in Netherlands, Philips, introduced the Philips Blockchain Lab as reported by www.coindesk.com. Information on the work they are doing in healthcare is not easily retrievable, but their collaborations with smaller companies specialising in blockchain have been made public. For example, Gem has said it is working with Philips to explore *"how blockchain technology can support a patient centric approach to healthcare*", according to www.gem.co, the company's official website. Medcitynews.com reports that Merk, a healthcare giant, is also exploring blockchain.

Around the world, research institutions are beginning to establish blockchain laboratories in response to the growing interest in the topic. For example, the Institute for the Future[12], University of Oulu, University College London and MIT Media Lab, have all recently established research work in the field. In Taiwan, TRPMA Biopharma Trusted Platform[13], is an initiative to connect researchers in academia to the industry, using blockchain technology for notary services and data traceability.

These are just a few examples; there seem to be dozens of small start-ups looking to use blockchain in different ways, especially in healthcare. The euphoria is clear; several blockchain advocacy, evangelists and associations are emerging the world over (see World Economic Forum whitepaper[14]). Looked at in total however, much of the work in big corporations and research institutions seems only exploratory and still pre-mature for evaluation.

4.5 National implementations and government initiatives

One the most talked about examples is Estonia, where they have used blockchain to verify and secure their public registries such as electronic health journals, judicial and legislative systems (see e-estonia.com and guardtime.com, the company behind the implementation). Estonia is arguably one of the leading eGovernment societies in the world, and they adopted blockchain for testing in 2008 and by 2012 the technology was put into routine use.

United Arab Emirates is another country taking blockchain seriously at a government level. According to the Wall Street Journal, IBM is their "*blockchain lead strategic partner*"[15]. The article reports that testing had already begun in 2017, with a goal of complete eGovernment services and transactions using blockchain by 2020. Guardtime and a telecom company partnered with the largest private healthcare provider in Dubai to use blockchain with their electronic health records, as reported recently by thenational.ae. These large scale initiatives by governments are not just targeted at healthcare but at a full array of electronic services offered by the governments. There are several blockchain initiatives passing through legislation in individual states such as Illinois and Delaware in USA.

---

[10] https://developer.ibm.com/blockchain/

[11] https://www.ibm.com/internet-of-things/platform/private-blockchain/

[12] http://www.iftf.org/blockchainfutureslab/

[13] www.trpma.org.tw

[14] http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf

[15] https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080

4.6 What are the knowledge gaps and challenges?

There is a wide range of questions that seem unanswered or that are only partially answered; philosophical, ethical, moral, legal, organisational and technical. Some of the challenges listed in this subsection could form the basis for scientific research, and the list is by no means exhaustive.

Philosophy: one of the main tenets of blockchain is the removal of trusted third parties, establishing a distributed public record of tamper-proof transactions. At its core is the "rebel" attitude that the community collectively create the whole, not the government or its agencies; no one party regulates what happens to the common resources, openness and transparency, yet preserving privacy and security of individuals. Research should ask whether patients want the ability to have granular control over how their data are used, for example in health registries. What kind of patients prefer to have a trusted third party, like government, make decisions on their behalf? Do patients have the ability to manage their data, including security peculiarities related to managing their private keys? Do positive use-cases outweigh negative consequences and harms?

Organisational: because of computational and privacy considerations, there is a general consensus that health data cannot be kept on a public blockchain, but only references to the data. One possible solution widely discussed, is the use of private blockchain (permissioned ledgers) where a consortium of healthcare providers use smart contracts. A disadvantage of this approach could be that private solutions normally result in vendor lock-in, which threatens openness. What sort of investment is required for existing and legacy systems to integrate with a blockchain? What incentives do vendors have to develop blockchain support? Does blockchain threaten the relevance of vendor systems in the future? What governance models can protect patients and provide legal recourse?

Technical: there have been proposals that the incentive for mining in a healthcare blockchain could be access to data [25]. For example, researchers would join the network as miners in order to gain access to health data. Is proof-of-work mining necessary for closed consortiums? Without mining and the idea of a trust-less network, is it still blockchain? Can a blockchain network really scale for healthcare use? What are the usability problems? How can user-friendliness be improved so that the average user can understand and participate?

5 Conclusion

Even though current understanding of the implications of blockchain is still limited, early research findings suggests the technology holds the promise of improving security and privacy, research and public health, and general health data management. Since research is still in its infancy, potential benefits, harms, challenges and questions, can be explored through more rigorous scientific inquiry.

After this report, a natural next step could involve planning for evaluation of the few known implementation cases, such as in Estonia and Dubai. This assures Norway's participation in related scholarly debate on issues of global interest. Alternatively, the next steps could involve forming limited consortiums to pilot parts of blockchain in isolated sandboxes.

In addition to technical questions, some areas where piloting could provide important knowledge include (i) qualitative surveys about patient willingness and ability to fully participate in managing their own health data (ii) how legacy healthcare systems could integrate with blockchain, and how blockchain infrastructures could be organised and governed to protect patients, and (iii) evaluating the potential benefits and harms. As part of the piloting, site visits and collaboration with large scale implementations could strengthen the research.

Even with seemingly insurmountable challenges, it appears unlikely the new trend with cryptocurrencies will disappear, but it is conceivable that major changes, both regulatory and technical, will take place before blockchain becomes more mainstream.

6 References

1. Antonopoulos, A.M., *Mastering Bitcoin*2014: O'Reilly.
2. Underwood, S., *Blockchain beyond bitcoin.* Commun. ACM, 2016. **59**(11): p. 15-17.
3. Extance, A., *The future of cryptocurrencies: Bitcoin and beyond.* Nature, 2015. **526**(7571): p. 21-3.
4. Sutherland, W.J., et al., *A 2017 Horizon Scan of Emerging Issues for Global Conservation and Biological Diversity.* Trends Ecol Evol, 2017. **32**(1): p. 31-40.
5. Yli-Huumo, J., et al., *Where Is Current Research on Blockchain Technology?—A Systematic Review.* PLoS One, 2016. **11**(10): p. e0163477.
6. Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system*.
7. Narayanan, A., et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*2016: Princeton University Press.
8. Irving, G. and J. Holden, *How blockchain-timestamped protocols could improve the trustworthiness of medical science [version 3; referees: 3 approved, 1 not approved]*. Vol. 5. 2017.
9. Zhao, H., et al. *Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys*. in *Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on*. 2017. IEEE.
10. Benchoufi, M. and P. Ravaud, *Blockchain technology for improving clinical research quality.* Trials, 2017. **18**(1): p. 335.
11. Nugent, T., D. Upton, and M. Cimpoesu, *Improving data transparency in clinical trials using blockchain smart contracts.* F1000Res, 2016. **5**: p. 2541.
12. Skiba, D.J., *The Potential of Blockchain in Education and Health Care.* Nurs Educ Perspect, 2017. **38**(4): p. 220-221.
13. Mettler, M. *Blockchain technology in healthcare: The revolution starts here*. in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. 2016. IEEE.
14. McKernan, K.J., *The chloroplast genome hidden in plain sight, open access publishing and anti-fragile distributed data sources.* Mitochondrial DNA A DNA Mapp Seq Anal, 2016. **27**(6): p. 4518-4519.
15. Hoy, M.B., *An Introduction to the Blockchain and Its Implications for Libraries and Medicine.* Med Ref Serv Q, 2017. **36**(3): p. 273-279.
16. Salahuddin, M.A., et al., *Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare.* Computer, 2017. **50**(7): p. 74-79.
17. Zhang, J., N. Xue, and X. Huang, *A Secure System For Pervasive Social Network-Based Healthcare.* IEEE Access, 2016. **4**: p. 9239-9250.
18. Hashemi, S.H., et al. *World of Empowered IoT Users*. in *Internet-of-Things Design and Implementation (IoTDI), 2016 IEEE First International Conference on*. 2016. IEEE.
19. Smith, K. and G. Dhillon, *Blockchain for Digital Crime Prevention: The Case of Health Informatics.* 2017.
20. Roehrs, A., C.A. da Costa, and R. da Rosa Righi, *OmniPHR: A distributed architecture model to integrate personal health records.* J Biomed Inform, 2017. **71**: p. 70-81.
21. Zhang, P., et al., *Applying Software Patterns to Address Interoperability in Blockchain-based Healthcare Apps.* arXiv preprint arXiv:1706.03700, 2017.
22. Yue, X., et al., *Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control.* J Med Syst, 2016. **40**(10): p. 218.
23. Ichikawa, D., M. Kashiyama, and T. Ueno, *Tamper-Resistant Mobile Health Using Blockchain Technology.* JMIR Mhealth Uhealth, 2017. **5**(7): p. e111.
24. Xia, Q., et al., *MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain.* IEEE Access, 2017.
25. Azaria, A., et al. *Medrec: Using blockchain for medical data access and permission management*. in *Open and Big Data (OBD), International Conference on*. 2016. IEEE.
26. Barratt, M.J., et al., *'What if you live on top of a bakery and you like cakes?'-Drug use and harm trajectories before, during and after the emergence of Silk Road.* Int J Drug Policy, 2016. **35**: p. 50-7.
27. Van Hout, M.C. and T. Bingham, *Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading.* Int J Drug Policy, 2014. **25**(2): p. 183-9.
28. Masoni, M., M.R. Guelfi, and G.F. Gensini, *Darknet and bitcoin, the obscure and anonymous side of the internet in healthcare.* Technol Health Care, 2016. **24**(6): p. 969-972.
29. Portnoff, R.S., et al. *Backpage and Bitcoin: Uncovering Human Traffickers*. in *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. 2017. ACM.
30. Mackey, T.K. and G. Nayyar, *A review of existing and emerging digital technologies to combat the global trade in fake medicines.* Expert Opin Drug Saf, 2017. **16**(5): p. 587-602.
31. Nugent, T., D. Upton, and M. Cimpoesu, *Improving data transparency in clinical trials using blockchain smart contracts.* F1000Research, 2016. **5**.