Doctoral theses at NTNU, 2023:121

Anton Hasselgren

Blockchain for trust and transparency in health information systems

Doctoral thesis

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of
Philosophiae Doctor
Faculty of Medicine and Health Sciences
Department of Neuromedicine and Movement
Science

NTNU
Norwegian University of
Science and Technology

Anton Hasselgren

Blockchain for trust and transparency in health information systems

Thesis for the Degree of Philosophiae Doctor

Trondheim, April 2023

Norwegian University of Science and Technology
Faculty of Medicine and Health Sciences
Department of Neuromedicine and Movement Science

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Medicine and Health Sciences
Department of Neuromedicine and Movement Science

ISBN 978-82-326-6273-9 (printed ver.)
ISBN 978-82-326-6150-3 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2023:121

Printed by NTNU Grafisk senter

Populærvitenskapelig sammendrag

Forskningen som presenteres i avhandlingen undersøker om blokkjedeteknologi kan være nyttig i helsesektoren. Blokkjedeteknologi ble først introdusert i kryptovaluta i 2008 og har siden blitt applisert på nye bruksområder, fra finansapplikasjoner til transport verdikjeder. Det her prosjektet utforsket om teknologien også kunne bidra med verdi innenfor helsesektor og dess applikasjoner. Forskningen er tverrfaglig og krysser helsevitenskap, informasjonsteknologi, datavitenskap og kryptografi.

Det er per i dag utfordringer knyttet til tillit, tilgangskontroll, innsyn og sporbarhet av data i mange helseinformasjonsystem. Blokkjedeteknologien har innebygde egenskaper som kan løse disse utfordringene, for eksempel data sporbarhet og data integritet. Av den anledningen er det interessant å se nærmere på om teknologiene kan bidra i noen bruksområder i den her sektoren. Målet med prosjektet var å undersøke bruken av blokkjedeteknologi i helseinformasjonsystemer og å utvikle en e-helse tjeneste som bruker en blokkjedeteknologi og evaluerer denne tjenesten.

Forskningen er basert på en problemorientert tilnærming, og inkluderer tre studier: en systematisk litteraturgjennomgang, en konseptstudie og en gjennomførbarhetsstudie. Den systematiske litteraturgjennomgangen avdekket viste at blokkjedeteknologi var blitt testet ut på områdene elektronisk pasientjournal og personlig helsejournal, men ingen av løsningene var tatt i bruk i klinisk praksis.

Konseptstudien bygde på en problemstillingen om det er muligt å øke tillit mellan helsepersonell og pasient i en virtuell helsekontekst med hjelp av applikasjon som bruker blokkjedeteknologi. Løsningen til den problemstillingen ble en desentralisert applikasjon for lagring av bevis på kompetanse, dette som en digital portefølje som helsepersonell kan bruke som dokumentasjon på hva de er i stand til å gjøre som helsepersonell. Applikasjonen hver bygd på en blokkjede for å kunne garantere ekthet og data sporbarhet. Gjennomførbarhetsstudien viste at brukere av systemet hadde en høy tiltro til den desentraliserte tjenesten.

Sammendraget viser resultatene i den her avhandlingen at blokkjedeteknologi kan være nyttig i en digitalisert helsesektor, spesielt når det gjelder å opprettholde tilliten mellom helsearbeidere og pasienter i et virtuelt miljø.

Abstract

Background

The research presented in this thesis explores whether the emerging technology of blockchain can provide value in the health domain. The research project is, in essence, interdisciplinary, migrating across health science, health informatics, computer science to cryptography. Challenges around trust, access control, data transparency and data provenance are present in health information systems and e-health applications. The emerging blockchain technology encapsulates inherited characteristics that provide data transparency, tamper-proof, integrity, and provenance. Exploring whether blockchain technology can provide any value to these challenges and the health system as a whole, is therefore of interest. The research project aimed to explore the topic of blockchain applications in health information systems. The aim extended to the design and development of an e-health related service that utilizes blockchain properties and evaluates that service.

Methods

This research work has adopted a problem-driven approach, and is based on design science and user-centered design theory. Three studies were undertaken in the scope of the research; a systematic literature review, a proof-of-concept study and a feasibility study.

Results

Systematic literature review: 39 publications were included in the review after screening based on strict inclusion criteria. The result indicates that Electronic Health Records and Personal Health Records are the areas most targeted by blockchain technology. Access control, interoperability, provenance and data integrity are all issues blockchain technology should be able to improve in this field. Ethereum and Hyperledger fabric seem to be the most used platforms/frameworks in this domain.

Proof-of-concept: This study determined and defined the crucial functional and non-functional requirements and principles for enhancing trust between caregivers and patients within a virtualized health care environment. The cornerstone of the architecture was a blockchain technology utilization approach. The proposed decentralized system provides an innovative governance structure for a novel trust model, and the presented theoretical design principles are supported by a concrete implementation of an Ethereum-based platform named VerifyMed.

Feasibility study: Five themes were identified from the interviews and focus groups held with real users of the system, after they were exposed to a mock-up of VerifyMed: (1) the need for aggregated storage of work and study-related verification, (2) trust in a virtual health care environment, (3) the potential use of patient feedback, (4) trust in blockchain technology, and (5) improvements of the VerifyMed concept. The System Usability Score questionnaire gave a score of 69.7.

Discussion

It is essential to systematically explore the digital transformation that is stimulated by new technologies, and their potential impact on health systems. Following a development cycle founded in design science, increases the development of a high-quality and fit-for-purpose system. The results from the feasibility study indicate that VerifyMed has a high degree of fit-for-purpose. System users expressed that a decentralized system for the storage of work-related verifiable credentials could increase trust in the health system, particularly where there are fewer trusted institutions as a result of an increase in the number of health care providers in a digitally transformed healthcare system. An advantage of this research project is the interdisciplinary approach to the multi-leveled topic of blockchain in health information systems. The VerifyMed project should advance to the next steps in the development cycle applied to this project, these being the development of an updated prototype based on the feasibility study's input, and testing the effect with real users. It is likely, where health services are provided in a virtual environment, that blockchain will provide value in digital transformed health systems. A decentralized technology that can guarantee data provenance and integrity could provide significant value to the maintenance of trust in a future in which physical interaction decrease.

Acknowledgements

This study was carried out at the Medical Faculty, the Norwegian University of Science and Technology (NTNU). Funding was provided by NTNU through the digital transformation research initiative, and I am very grateful to NTNU for the opportunity to deep dive into this exciting research field. Secondly and perhaps most importantly I would like to express my gratitude towards my supervisors Professor Arild Faxvaag at the Department of Neuromedicine and Movement Science, NTNU, and Associate Professor Katina Kralevska and Professor Danilo Gligoroski at the Department of Information Security and Communication Technology, NTNU, who have guided me through this work. I would also like to express my appreciation of the collaboration with my fellow PhD colleagues and their respective supervisors in the digital transformation project. My thanks must also go to the participants in this research, who contributed their perspectives and suggestions.

Contents

List of Figures

List of Tables

List of Publications

Paper A

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S.A. and Faxvaag, A., 2020. Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, p.104040.

Paper B

Hasselgren, A., Rensaa, J.A.H., Kralevska, K., Gligoroski, D. and Faxvaag, A., 2021. Blockchain for increased trust in virtual health care: proof-of-concept study. Journal of Medical Internet Research, 23(7), p.e28496.

Paper C

Hasselgren, A., Kralevska, K., Gligoroski, D. and Faxvaag, A., 2021. Medical Students' Perceptions of a Blockchain-Based Decentralized Work History and Credentials Portfolio: Qualitative Feasibility Study. JMIR Formative Research, 5(10), p.e33113.

Authors' roles and contributions

Paper A Anton Hasselgren contributed to the conceptualization, methodology, visualization, writing, and original draft preparation of the paper. The original search was done by Sindre A. Pedersen with a search strategy developed together with Anton Hasselgren. Katina Kralevska contributed to the writing, reviewing, supervision, and conceptualization. Danilo Gligoroski contributed to the writing, reviewing, supervision, and conceptualization. Arild Faxvaag was involved with the conceptualization, methodology, visualization, writing, reviewing, and supervision.

Paper B Anton Hasselgren contributed to the conceptualization, methodology, visualization, writing, and original draft preparation of the paper. Jens-Andreas Hanseen Rensaa contributed to the data curation, software, and visualization. Katina Kralevska contributed to the writing, reviewing, supervision, and conceptualization. Danilo Gligoroski contributed to the writing, reviewing, supervision, visualization, and conceptualization. Arild Faxvaag contributed to conceptualization, methodology, visualization, writing, reviewing, and supervision.

Paper C Anton Hasselgren contributed to the conceptualization, methodology, visualization, writing, and original draft preparation of the paper. Katina Kralevska contributed with reviewing and supervision. Danilo Gligoroski contributed with reviewing and supervision. Arild Faxvaag contributed with reviewing and supervision.

Additional publications of relevance

Paper 1 Rensaa, J.A.H., Gligoroski, D., Kralevska, K., Hasselgren, A. and Faxvaag, A., 2020, July. VerifyMed-A blockchain platform for transparent trust in virtualized healthcare: Proof-of-concept. In Proceedings of the 2020 2nd International Electronics Communication Conference, pp. 73-80.

Paper 2 Hasselgren, A., Wan, P.K., Horn, M., Kralevska, K., Gligoroski, D. and Faxvaag, A., 2020, October. GDPR Compliance for Blockchain Applications in Healthcare. In Proceedings of the International Conference on Big Data, IOT and Blockchain (BIBC 2020), Dubai, UAE, pp. 24-25.

Paper 3 Platt, M., Hasselgren, A., Román-Belmonte, J.M., De Oliveira, M.T., De la Corte-Rodríguez, H., Olabarriaga, S.D., Rodríguez-Merchán, E.C. and Mackey, T.K., 2021, December. Test, Trace, and Put on the Blockchain?: A Viewpoint Evaluating the Use of Decentralized Systems for Algorithmic Contact Tracing to Combat a Global Pandemic. JMIR Public Health and Surveillance, 7(4), p.e26460.

Paper 4 Satybaldy, A., Hasselgren, A., Nowostawski, M., 2022, Mars. Decentralized Identity Management for E-Health Applications: State-of-the-Art and Guidance for Future Work. Blockchain in Healthcare Today, 5(S1).

Paper 5 Hasselgren, A., Wu, S. and Jiang Galteland, Y., 2022. Cryptographic Tokens as an Incentive Mechanism for Patient-reported Outcome Measures Surveys: a proof-of-concept. JMIR Preprints. 24/01/2022:36752

List of Abbreviations

AI - Artificial Intelligence
DeFi - Decentralized Finance
ECDSA - Elliptic Curve Digital Signature Algorithm
EHR - Electronic Health Record
FDA - U.S Food and Drug Administration
GDPR - General Data Protection Regulations
HIPAA - American Health Insurance Portability and Accountability Act
HIS - Health Information System
ICT - Information and Communications Technology
IoT - Internet of Things
NTNU - The Norwegian University of Science and Technology
UX - User Experience
PBFT - Practical Byzantine Fault Tolerance
PoC - Proof-of-Concept
PoS - Proof-of-Stake
PoW - Proof-of-Work
PRO - Patient Reported Outcome
PREMs - Patient Reported Experience Measures
PROMs - Patient Reported Outcome Measures
SUS - System Usability Scale

1 Introduction

The research presented in this thesis explores whether emerging blockchain technology can provide value in the health domain. This research work is, in essence, interdisciplinary. It extends across the boundaries of health science, health informatics, computer science and into cryptography. It is, furthermore, under the umbrella of the Digital Transformation research initiative at the Norwegian University of Science and Technology (NTNU) [1]. The motivation spurring this research work lies in the challenges that threaten health systems, such as a growing elderly population, a consequent increase in highly demanding chronic diseases [2], a shortage of healthcare professionals [3] and a lack of sufficient financial resources [4]. These challenges need to be met if health systems are to be able to continue to achieve their overall goals of improving health, legitimate responsiveness to population expectations, and fairness in financial contributions [5]. New digital technologies introduced into the health domain could bring profound changes that can improve quality and reduce costs [6]. Blockchain, first introduced in the Bitcoin cryptocurrency [7], has been suggested of having the potential to have a profound impact in the health domain [8]. The exploration of whether blockchain has a place in the digital transformation of the health sector is therefore of vital importance.

The philosophic position of this research work is tended towards positivism, which assumes a single reality that can be objectively measured. This seems to be the predominant philosophical approach in health informatics and information systems in electronic health records research, which is related to this research work [9]. Therefore, the work has been carried out based on the research tradition of health information systems with roots from the discipline of evidence-based medicines and a philosophical approach of positivism. Methods, theory and overall research approach are from the research tradition of health information systems. Although, methods and knowledge from other disciplines have been integrated. When theory and methods from other disciplines were applied, they were adopted to fit in the scope of health information systems research tradition. This perspective was chosen based on the author's background, the attachment to the faculty of medicine at NTNU and the importance of exploring technology with a domain lens. The interdisciplinary approach has been a crucial component in exploring this new technology from both a domain and a technical perspective. Figure 1.1 illustrates the interdisciplinary nature of the work, and how it relates to a number of academic disciplines. The figure is a simplified illustration of a reality that is more complex and consists of more sub-areas.

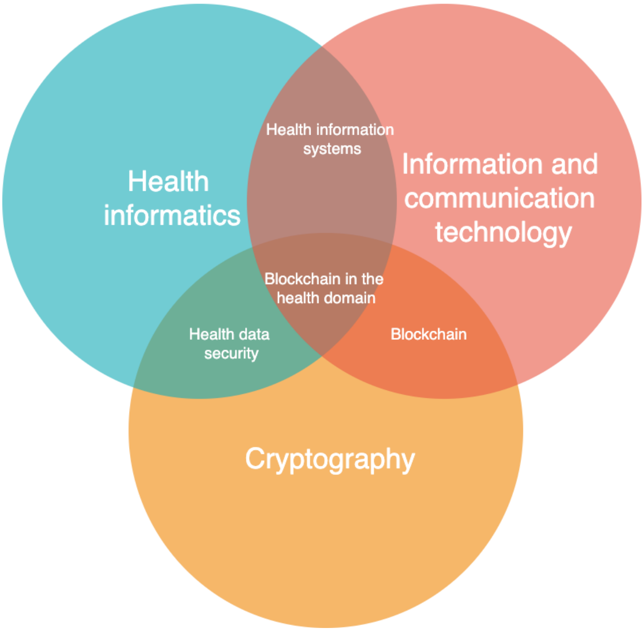


Figure 1.1: Interdisciplinary illustration of blockchain in healthcare

This dissertation thesis is synthesized from three research studies published in academic journals [10, 11, 12]. The thesis summarizes these studies, but also provides an overview of the project, the theoretical and methodological approach and gives a more in-depth discussion of the results as a whole. The dissertation thesis is organized as follows: **Section 2** provides the background to the research field and important concepts and definitions within cryptography and healthcare informatics. These are provided to facilitate reader comprehension of the remainder of the thesis, **Section 3** outlines the aim and objectives of the research project, **Section 4** describes the theoretical foundation which serves as a basis for the research approach, **Section 5** outlines the main contributions of the three studies and **Section 6** provides a discussion of the main contributions and the research project as a whole.

2 Background

This chapter defines and describes the central components of digital transformation, health information systems (HIS), blockchain, and related concepts and terms. These are all very broad topics, and an explanation of them could fill many books. The scope of this chapter has, however, been limited to providing the necessary definition and background information to the reader, to allow the comprehension of the objectives, research approach, and methodology of this research project.

2.1 Digital transformation

Digital transformation can be defined as the profound changes taking place in the society and industries through the use of digital technologies [6, 13]. The term digitalization is often used in the same context and can be described as the application and use of digital technologies throughout society [14]. Thus, the distinction between the two terms is the profound changes in the society that the transformation brings. Digitization, which is often used interchangeably with digitalization, has a slightly narrower definition. It can be defined as being the shift from existing analog products or services into digital formats [14], the term therefore does not include digital services or products which introduce new functionality. The introduction of electronic health records (EHR) in the early 90s is an example of digitization: the EHRs merely moved the paper-based system to a digital format, without adding any new functionality [15]. On the other hand, the introduction of a variety of health apps that often allow the patients to track and analyze their health condition in a manner that has not been possible or feasible previously, can be described as digitalization [16].

What can be categorized as "profound changes" can be debated. Digitalization in health systems is, however, changing the way health services are delivered [17], evaluated and financed [18]. New digital tools also allow disease prevention, health promotion, and early detection of diseases [19]. These can be considered to be profound changes in health systems. This therefore represents the digital transformation of health systems. The digital transformation in health systems can also include, but is not limited to, the implementation of new digital services such as health information websites, online self-management tools and personal medical records. These services can provide patients and citizens with a higher degree of control and management of their health, which has not been feasible previously, therefore introducing profound changes to health systems [20].

Matt et al., dissecting further what "profound changes" could entail, describe four universal, essential dimensions of digital transformation that apply irrespective of industry. These are use of technologies, changes in value creation, structural changes, and financial aspects [21]. Blockchain technology can, as described later in this work, address all four of these dimensions in a number of industries, including the health domain. This technology could serve in the health sector as an active component of digital transformation. The transformation potential of blockchain in the health domain, has not been adequately explored in the literature prior to this research work. It has previously only been suggested as a potential technology. This is further described under blockchain in the healthcare section.

What drives the digital transformation in health systems is also a topic of debate. Suggested drivers of digital transformation in society as a whole include customer behavior and expectations, digital shifts in industry, changing competitive landscapes and regulative changes [22]. This can be translated in the health domain to a change in patient behavior and expectations, new digital technologies such as patient-centered mobile applications, new digital healthcare providers, and changes in health regulations. The health sector is, as a result of these drivers, transforming into a digital and data-driven domain. Infrastructures such as electronic health records (EHR), electronic prescriptions and information portals, which are often associated with the digitalization of the sector [23], could bring about profound changes to the system. Recent technologies such as mobile health applications with the patient as end-user, which allow the patient to take a greater degree of control over their health and diseases than before, have rapidly emerged and are perhaps making a more significant contribution to the profound changes witnessed [16]. Digital transformation implies the application of digital technologies. HIS is presented as an umbrella of digital data technologies in health systems in the next section.

2.2 Health information systems

A good starting point for understanding HIS is taking a broader perspective, looking at health systems as a whole and the importance, functions and challenges associated with these systems. A health system can be defined as being: "The system that comprises all organizations, institutions and resources that produce actions whose primary purpose is to improve health" [24, p. XI]. Healthcare system is defined more narrowly as the institutions, people and resources involved in delivering healthcare services to individuals [24]. This thesis primarily focuses on the broader health systems concept.

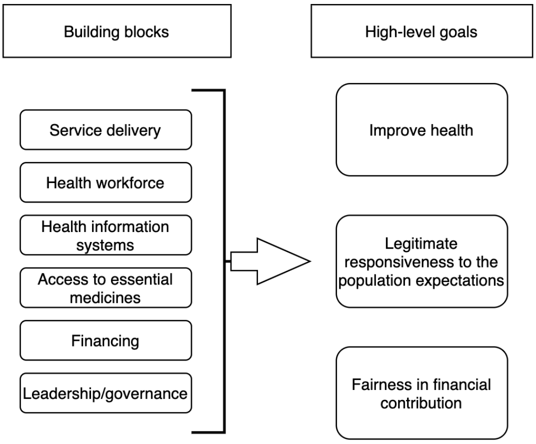


Figure 2.1: Building blocks of a health system and the overall goals, adopted from [25, p. 7]

Health systems can be described as having three high-level main goals: improving health, legitimate responsiveness to the population's expectations and fairness in financial contribution. These goals can furthermore be broken down into instrumental goals for measuring performance, such as access to care, community involvement, innovation, or sustainability. They all, however, tie back to the three high-level goals [5].

Health systems can be described as having six core building blocks, which all contribute to the strengthening of the system and to the fulfilment of the high-level goals of: (i) service delivery, (ii) health workforce, (iii) health information systems, (iv) access to essential medicines, (v) financing, and (vi) leadership/governance [25]. These blocks can be stratified into three categories: overall policy and regulation (HIS and leadership/governance), input components (financing and the health workforce) and output components (medical products, technologies and service delivery). These categories and the building blocks are, in some instances, intertwined. For example, patient and citizen privacy both relate to the governance block, which in turn relates to the field of data protection laws and regulations. The role of the health information system is to ensure that these regulations are followed. All health systems face challenges with the design, implementation, evaluation, and reformation of the organizations and institutions that facilitate these building blocks [26]. This thesis does not attempt to cover these building blocks, merely highlighting the role of health information systems as a key component in health systems, which is of relevance for the scope of this research project.

HIS can be defined as a system that integrates data collection, processing, reporting, and use of the information necessary for improving health service effectiveness and efficiency through better management at all levels of health services [27]. It encompasses all health data sources including (but not limited to): health facility and community data, electronic health records for patient care, population-based data, human resources information, financial information, supply chain information, surveillance information, and the use and communication of this data [27]. HIS can be described as having four high-level functions: (i) data generation, (ii) compilation, (iii) analysis and synthesis, and (iv) communication and use [25]. Tools used in these functions include, for example, clinical guidelines, decision support systems, electronic records, communication systems and mobile applications. These functions and tools are, as for HIS as a whole, only a means to the end of contributing to the goals of the health system [28]. The functions of HIS need to achieve the HIS objectives, and at the same time comply with governance frameworks such as health data regulations and laws. HIS can, as an extension of these sub-functions, be defined as performing the above-mentioned functions while protecting the data privacy of the actors involved in the system.

Recent examples of health information system failure include large data breaches and the theft of patient-related data, and even this being held for ransom [29]. This seems to be more common in the USA than Europe, perhaps due to the difference in the regulation frameworks of the two continents [30]. New developments in HIS need to take this into consideration, to ensure data infrastructure complies with current regulations, and meets the fundamental information security goals of confidentiality, integrity, and availability [31].

The quantity and quality of health data is expanding rapidly, and new data sources such as personal health data, often gained through personal health trackers, have emerged. HIS therefore becomes of an increasing importance to meeting the goals of the health system, as illustrated in Figure 2.1.

2.2.1 E-health

The term e-health started to appear with the adoption of digital technologies and Internet in the late 1990s. It was used to refer to Information and Communication Technologies (ICT) solutions that could improve elements of health systems, such as EHR systems [32]. Eysenbach defined e-health in 2001 as: "an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through Internet and related technologies" [33, p.1]. The term, in a broader sense, characterizes not only the technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment to networked, global thinking, to improve healthcare locally, regionally, and worldwide using information and communication technology [33]. This broad definition of e-health is similar to the definition of HIS. The distinction is that HIS does not necessarily require Internet or related technologies, nor digital technologies, despite most HIS having at least some digital components. A broad definition of e-health and HIS therefore often refers to the same primary components.

Some suggestions of less broad definitions have, however, been made such as this by Fonseca et al: "E-health can be defined as a set of technologies applied with the help of Internet, in which healthcare services are provided to improve quality of life and facilitate healthcare delivery." [34, p. 1]. E-health can be considered, in this narrower definition, to be a sub-field of HIS. Choosing between a wide and narrow definition of e-health is not of significance to this work. What is important, however, is that narrow and broad definitions of e-health both imply that patients and healthcare professionals are essential users of the technology. They should therefore be involved in the design, implementation, and evaluation of e-health interventions. It was evident in the early days of e-health that poor usability can be a significant obstacle to new technology acceptance in the healthcare sector, if not appropriately designed with the involvement of end-users [35]. More recent studies indicate that this still is a significant issue [35]. ICT-based health interventions or health services can, furthermore, be a substitute for traditional methods of healthcare delivery, and have even been shown to potentially be more effective [36].

E-service has been widely adopted in other domains as a part of digitalization. Such e-services can be defined as: deeds, efforts or performances whose delivery is mediated by information technology (including the web, information kiosks and mobile devices) [37]. This approach is therefore equally important to technology interventions in HIS.

COVID-19 presented unprecedented challenges to health systems across the globe. Digital transformation in healthcare faced a rapid acceleration in this period, as physical meetings were reduced. Virtual health care consultations, often referred to as telemedicine, played an active role in the digital transformation during this period. It provided a new means of healthcare delivery that reduces barriers such as the lack of availability and lack of access, and through this has a profound impact on peoples' health. An example of digital transformation accelerating due to COVID-19 is the increase in virtual health care consultations by 683% in New York City through the spring of 2020 [17]. General practitioners in Norway also reported that 81% used video consultation during the pandemic (most not using it at all before the pandemic) [38].

The concept of a learning health system was introduced with the increase in health-related data. Learning health system has been described as: "harness the power of data and analytic to learn from every patient and feed the knowledge of ’what works best’ back to clinicians, public health professionals, patients, and other stakeholders to create cycles of continuous improvement" [39, p. 44]. Patient-reported outcomes (PROs) could be a vital part of the learning health system, providing a direct feedback loop from patients. PROs is described as a concept in the next section.

2.2.2 Patient-reported outcome measures

The concept proposed and developed in this research, utilizes patient-reported outcome measures (PROMs) as an essential component of the verification of the competence of healthcare professionals, and as a learning mechanism. The section below therefore introduces PROMs as a concept and the definitions used throughout this research.

A central element of gaining new knowledge in a health system and achieving a learning health system, is learning from the results of given health services. This can be achieved by obtaining outcome measures from that care [40]. Medical devices can measure outcomes as biomedical conditions. Some outcome measures can, however, only be collected by asking the patient. These are referred to as patient-reported outcomes (PROs), and have been proposed as a measure for collecting data and gaining knowledge and this measure has previously been lacking [41]. The definition of PROs tends to vary. This project has, however, adopted the following definition of the US Food and Drug Administration (FDA): "PRO is any report of the status of a patient’s health condition that comes directly from the patient, without interpretation of the patient’s response by a clinician or anyone else" [42, p. 1].

PROs can be obtained through the use of patient-reported outcome measures (PROMs) and also through the less used patient-reported experience measures (PREMs). PREMs measure the experiences of health services, and often use satisfactory standardized scores [43]. PROMs are usually multi-dimensional, and measure the quality of life; the EQ-5D questionnaire is currently one of the tools most used to obtain this data [44]. However, PROMs can also be one-dimensional and focus on specific health conditions or disease outcomes. Systematic use of PROs in clinical and research practice can give accurate and comprehensive data on patient experiences and outcomes. This can also add to the overall knowledge of outcomes of specific health services and treatments [45]. PROMs surveys often today use a digital format, the electronic follow-up providing an opportunity to improve communication with the patient. It has also been suggested that this can reduce costs compared with pen and paper surveys [46].

2.3 Challenges facing health information systems

The growing field of health-related data is a component that relates to HIS and this work, and encompasses all of the mentioned driving factors of digital transformation. Health-related data, which includes patient-level data, has expanded exponentially in the last decade [47]. Health-related data can act as a catalyst of digital transformation, the data having the capacity to bring profound changes in how healthcare is organized, delivered and evaluated. This data also, however, presents some major challenges. The variety of this data extends, but is not limited to; patient demographics, encounters, diagnosis, pathology, laboratory tests, medications, radiology, radiation treatments, surgical treatments, post-therapy care, notes and documents, operational, financial and insurance information, and provider characteristics. These data elements are scattered across the digital (and physical) sphere, making the aggregation of this data challenging. The data also is often unstructured, especially data from EHR systems [48]. This makes the software mining of data and enabling current machine learning algorithms to learn from the data difficult. The increase in health-related data can therefore be seen as both a catalyst of and a challenge to digital transformation.

Other challenges related to health data include: data access-control [32], data transparency, data security and data provenance [49]. There are also challenges within e-health applications (when considered a sub-field of HIS) including user-friendliness, conformity with the current regulatory framework, fit within the current technical infrastructure, interoperability, affordability, and user accessibility and communication issues [50]. User accessibility and communication issues can be tackled by adopting directions such as interactive communication, adaptions for all population groups, engaging the user, and a broad reach. The communication component should, to achieve this, have a high degree of trust and transparency, the data generated in these subsystems being trustworthy.

2.3.1 Trust in health systems

Trust is a concept which has a number of different definitions, the definition varying with academic discipline [51]. The trust concept is used, in this work, in the context of health science. The following definition has therefore been adopted: "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" [52, p. 395].

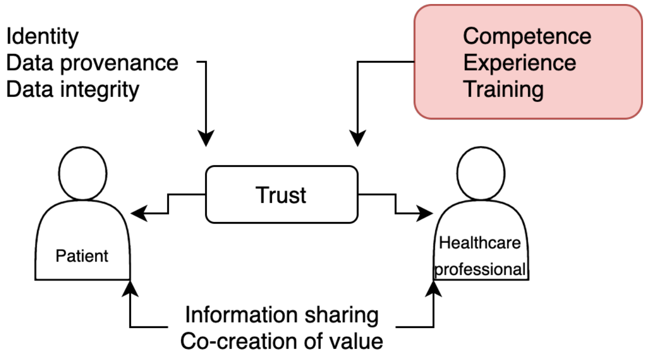


Figure 2.2: Factors influencing trust in a patient-caregiver interaction [11, p. 5]

Trust between a patient and a healthcare professional who delivers health services is, in clinical practice, a central component of quality care and core function of a physician's work is to establish and maintain trust with their patients in clinical practice [53]. Trust in these settings can be viewed from a human psychology perspective [54]. Patients must be able to trust doctors with their lives and health [55]. The same can be said about other healthcare professions, such as nursing [56].

Trust in healthcare professionals can furthermore be seen to be the foundation of the delivery of qualitative care [57], and a core component of patient-centered care [58]. The establishment and maintenance of this trust in the patient-physician interaction, is considered to increase treatment adherence, patient satisfaction, and improve health status [59].

Trust, from a human psychology perspective, can be categorized into interpersonal, social, and dispositional trust [60]. The trust in this project has mainly been an interpersonal trust. This is dependent on components such as the reliability (good reputation), competence (having the skills required to perform the task), and integrity (honesty) of the person in whom trust is placed [61]. Patients base the trust they place in a physician on characteristics such as competence, compassion, privacy and confidentiality, reliability, dependability, and communication skills [62].

The digital transformation of healthcare involves a continued increase in web-based consultations, as it was seen during the COVID-19 pandemic [17, 38]. The successful delivery of health services in this setting requires the co-creation of value between a healthcare professional and a patient [63]. It is crucial that patients actively participate in value creation, trust being an essential prerequisite. The factors of interpersonal trust foundation in healthcare professional-patient relationships are given in Figure 2.2.

It should be mentioned that trust in medical technologies is deeply intertwined with institutional trust and technical reliability [64]. Trust in new technologies such as blockchain, therefore needs to be understood if implementation is to be successful.

2.4 Blockchain

Blockchain can be categorized as an emerging technology [65, 66, 67]. The basic technical elements of blockchain are described in this subsection, to help the reader understand its potential in health systems and in this research work. Blockchain first gained attention with the introduction of bitcoin [7] and later Ethereum [68]. It was, at the time, widely speculated upon how this new technology could transform a wide range of industries, healthcare being one of the most prominent [8].

The definition of blockchain tends to vary across academic, regulatory and private spheres. The following definition has, however, been adopted in this work: "Blockchains are tamper-evident and tamper-resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government)" [65, p. ii].

This definition can be further dissected; Blockchain ledgers are data structures composed of a series of bundles of transactions. These bundles are called blocks, and contain transactions and other metadata. Blockchain network nodes create blocks based on their observed transactions. Network nodes apply consensus mechanisms and finally append the block to the blockchain ledger, linking it back to a previous block. Descriptions of transactions, of how blocks are composed, and how they are linked together are presented in this section. The Bitcoin blockchain ledger is used as shown in Figure 2.3, in the context of the examples presented. The cryptographic components vital for blockchain are first presented, the concept of transactions, blocks and chains are then introduced, and the distinctions between different blockchains are finally described.

The core cryptographic components of blockchain technology are introduced in the following subsections, to help the reader understand the technology. The technical aspects and this research discipline's perspective have not been the focus of this work. A basic understanding of the technology is, however, essential to fully understand the research presented in this project.

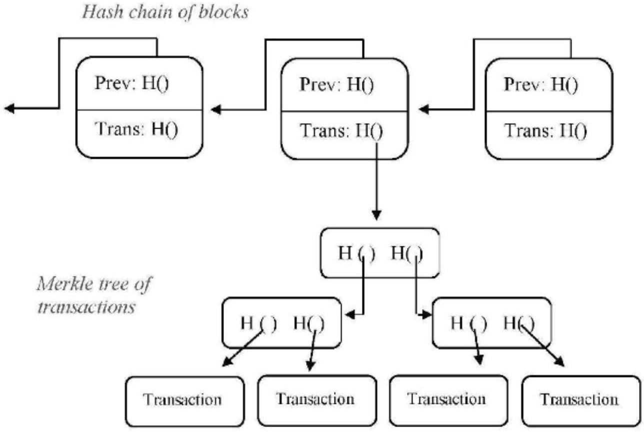


Figure 2.3: A hash list for calculating a root hash over a set of data [10, p. 2]

2.4.1 Hash Functions

Hash functions were introduced in the 1970s to ensure the authenticity of data. They are today a vital component of modern cryptography. Hash functions compress a string of arbitrary input into a string of fixed length [69]. Today's most used hash functions are the Secure Hash Algorithm (SHA) which, for example, the Ethereum blockchain uses [68]. Hash functions are a vital component of blockchains, the data in the blocks acting as the input (message), the output (digest) being included in the proceeding block and so forming a chain of blocks. This enables blockchain audit, traceability, and tamper-proofness.

2.4.2 Merkle Trees

Hash functions are, in blockchains, used in hash lists - mainly Merkle trees [70]. Data entries in the blocks are formed into a tree structure. Each leaf value can be verified to the known root hash, this method first being described in Merkle's 1982 patent [71]. It is therefore possible, given that the root hash is known, to recalculate the data in the blocks and compare the output with the root hash. If the hash output is equal to the root hash, then the verifier can be certain that the underlying data entries are equal. This allows the integrity of the data to be verified using only the root of the tree stored on the blockchain. Figure 2.3 provides a visualization of this basic structure.

2.4.3 Public Key Encryption

Another crucial component of blockchains is public key cryptography, which was first introduced in 1977 [72]. An asymmetric key pair is used for authentication and for confidentiality purposes. The key pair consists of a secret (private) key and a public key. The owner's secret key remains, as the name implies, secret. The public key is shared. The keys are used in most blockchains for digital signatures such as the Elliptic Curve Digital Signature Algorithm (ECDSA) [73]. Public key encryption enables, for example, the receiver of messages encrypted using a public key, to decrypt them using a pairing private key. This ensures that only the receiver can read the message, for example as in emails [74]. The sender can therefore ensure that only the secret key holder can view the message.

2.4.4 Smart Contracts

Smart contracts were first introduced by Nick Szabo in 1997 [75]. Placing smart contracts on an immutable ledger opens up a wide range of use-cases for decentralized technologies, and eliminates the need for a third party to validate a contract. Smart contracts in blockchains were first introduced in the Ethereum blockchain in 2014 [68], which is still the leading blockchain for the development of smart-contract applications. Similar and alternative public ledger technologies have, however, in the interim been proposed, such as Hyperledger [76] and Avalanche [77]. Distributed applications that are run using smart contracts on a blockchain are sometimes referred to as Dapps [78]. Smart contracts work in a way that is similar to classes in object-oriented languages. They have internal state, constructors, inheritance, and externally or internally accessible functions [78]. Smart contracts are stored as bytecode on the blockchain ledger, from where they get their address. This enables the contract function to be executed with a transaction. Smart contracts are primarily developed by the writing of code in a high-level language such as Solidity [79].

A smart contract is created by a user taking the compiled bytecode, and packing this into a contract creation transaction. The user signs the contract using their secret key, which allows the entire transaction to be composed. This transaction is then published on the blockchain platform by sending it to a node in the network, which validates its authenticity.

An address is assigned to the contract once a contract has been added to the blockchain ledger via a contract creation transaction. This address is not associated with a given key pair, is not deduced from key pairs, but is instead a calculated address which is under the control of the contract. The address is calculated by taking the last 160 bits of the Keccak hash of the encoded sending address, and nonce from the contract creation transaction [78].

Users must create a new contract invocation transaction to interact with a contract. This transaction contains bytecode that indicates which function is to be invoked in the smart contract, and function parameters. This interface can be created during the compilation of the contract, and describes how contract calls are encoded and decoded into bytecode.

2.4.4.1 Transactions

Transactions are data stored on the blockchain, in cryptocurrencies such as Bitcoin [7], transactions sending tokens from one account to another. Transactions can, however, also interact with the blockchain through smart contracts. It is possible, in blockchains that enable smart contracts, for transactions to invoke a large set of predefined processes, the payload in the transaction dictating which processes to invoke.

2.4.4.2 Blocks

Blocks are the set of transactions that are bundled into a block. Blocks of transactions are, in most blockchains, linearly tied to the blockchain. Network participants, through a consensus mechanism, approve which blocks are tied to the chain and through this approve which transactions (or data entries) are valid. Figure 2.3 uses a Merkle tree to create a root-hash of all transactions contained within the block. A prover who wants to show that a transaction was present in a given block, can use a Merkle tree proof to convince the verifier of this. The validity of a transaction that has been added to a block in the chain, cannot be disputed.

2.4.4.3 Chains

Chains are the link from one block to another, made by including the hash value of the previous block into the next block. Figure 2.3 is a visual representation of the chain in the Bitcoin ledger. The figure shows that the block header contains the hash of the previous block. The purpose of the chain is to create an order of blocks, and to provide tamper-proofness to the blockchain, through no data in previous blocks being able to be altered without changing the hash of the set block, which has already been included in the following block.

Table 2.1: Blockchain classification [67, p. 148557]

Blockchain Type	**Application Domain**	**Anonymity**	**Scalability**	**Challenges**	**References**
Permissionless Public	Decentralized P2P Networks	High	Low	Privacy, Scalability	Bitcoin [7], Zerocash [80], Monero [81]
Permissioned Public	Decentralized Organizations	High	Moderate	Privacy, Centralization	Ripple [82], EOS [83]
Permissionless Private	Intra-Organization Networks	Moderate	Moderate	Consensus, Scalability	LTO [84]
Permissioned Private	Organizational restricted ledgers	Low	High	Consensus, Centralization	Hyperledger fabric [85], Monax [86], Multichain [87]

2.4.5 Types of Blockchain

Blockchains can be classified by the characteristics and rules that define who can access, write and read the data on the blockchain. Standard classifications are "public" or "private," the classification terms "permissioned" and "permissionless" also being used. These terms are used interchangeably in most blockchain studies and industrial applications, which is a practice that can be questioned. The classification of blockchains is not clearly specified in the literature. Blockchains can, however, be classified by coupling public, private, permissioned and permissionless.

1. *Permissionless Public:* Anyone can participate in the network, the consensus procedures, and ledger maintenance of this type of blockchain. Everyone participating in the network can read and write to the blockchain, participants being provided with minimum trust, but maximum transparency. Most of the larger cryptocurrencies and blockchain platforms are permissionless public, e.g., Bitcoin [7], Ethereum [68] and Monero [81].

2. *Permissioned Public:* Everyone is allowed to read the data on this type of blockchain. Permission to write data and take part in consensus protocol are privileges that are granted by network administrators, meaning that the system is not fully decentralized. A participant in this type of blockchain who has been granted some privileges, can also become a validator. Examples of permissioned public blockchains are Ripple [82], EOS [83] and Libra [88].

3. *Permissionless Private:* This type of blockchain allows organizations to collaborate on a decentralized ledger, without having to share the information publicly. Permissionless means anyone can join or leave the blockchain at any time. The smart contracts on these blockchains can, however, be further defined to specify who has access to a specific contract. Some permissionless private blockchains use a Federated

Byzantine Agreement as consensus protocol. The LTO [84] network is an example of a permissionless private blockchain that creates "live contracts" on the network.

4. *Permissioned Private:* These blockchains are primarily used in organizations in which data/information is stored on the blockchain, permissioned access being controlled by members of the organization. The network administrator or a membership authority grants access to the network, and decides who can read and write data on the ledger. Hyperledger fabric [85], Monax [86], Multichain [87] are examples of permissioned private blockchains.

Table 2.1 provides an overview of the classification of blockchains and the associated advantages, challenges and application domains. Permissionless public blockchains are, in general, commonly referred to as public blockchains. Permissioned private blockchains are referred to, in general, as fully private blockchains. A combination of permissioned public and permissionless private gives a "consortium blockchain," which is also called a federated blockchain. A consortium blockchain is neither wholly public nor completely private, making this blockchain partially decentralized. Consensus is reached in a consortium blockchain by a selected group of participants. Most organizations today have embraced consortium blockchains for their blockchain-enabled solutions.

Table 2.1 illustrates the different blockchain architectures present and the associated centralization, immutability and efficiency trade-offs. This is sometimes referred to as "The blockchain trilemma" [89], which represents the significant trade-offs facing all blockchains. The table clearly shows that maximum simultaneous security, decentralization and scalability is unachievable, a trade-off between these three properties being unavoidable.

2.4.6 Consensus mechanisms

A predefined consensus protocol determines whether data entries are accepted onto the blockchain ledger. This protocol furthermore represents agreement across the network on the premises for data entry acceptance. There are a number of consensus mechanisms, some implemented in blockchains, others still in the research phase [90]. The three most common protocols currently are:

Proof-of-Work (PoW) is the most widely used consensus protocol and the one most strongly associated with blockchain, due to being integrated into the largest blockchain, Bitcoin and previously also in the second largest, Ethereum. PoW uses a computationally intensive puzzle which participating nodes in the blockchain network must solve to validate transactions, and for new blocks to be created using brute force. These nodes are referred to as miners, and the process is referred to as mining. The miner who first solves the puzzle for the next block, receives a reward in new-minted coins. The concept of PoW was first introduced in 1992 as a means of mitigating junk e-mail [91]. The term "proof of work" was, however, first introduced in 1999 [92]. A major drawback of the PoW protocol, and a common criticism of blockchains, is its energy consumption when applied to large blockchains such as Bitcoin. This is often illustrated by the electricity consumed by Bitcoin mining today being equivalent to the electricity requirement of a small country [93].

Proof of Stake (PoS) uses selected nodes for the verification and approval of transactions, based on the stake each node has in the blockchain. The stake for cryptocurrencies is the balance held in that currency. A number of hybrid versions of PoS have also been proposed, the stake being combined with randomization in the selection of the approving node. The second-largest cryptocurrency, Ethereum, has successfully moved from PoW to PoS in Ethereum 2.0 [94].

Practical Byzantine Fault Tolerance (PBFT) is based on a Byzantine agreement protocol, which was first introduced in 1999 [95]. PBFT requires all nodes to be known to the network, this hindering the application of this consensus protocol in a public blockchain. Each node needs two-thirds of the votes of all nodes to move through the three phases. PBFT is currently used in Hyperledger Fabric [96].

Table 2.2: Overview of consensus protocols, adopted from [97, p. 560]

Property	**PoW**	**PoS**	**PBFT**
Node management	Open	Open	Permissioned
Energy consumption	High	Medium	Low
Tolerated power of adversary	< 25% computing power	< 51% stake	< 33.3% faulty replicas
Example	Bitcoin [7]	Ppcoin [98]	Hyperledger Fabric [96]

2.5 Blockchain in healthcare

Blockchain in healthcare was still a relatively new research topic at the start of this research project in August 2018, and still is to some extent. Papers such as "Blockchain technology in healthcare: The revolution starts here" [8] and "Medrec: Using blockchain for medical data access and permission management" [99] were receiving attention at this time. These early papers proposed that the inherited characteristics of a blockchain (decentralization, transparency, provenance and accountability) might be a good fit-for-purpose with some of the challenges in health systems and HIS. They discussed blockchains' potential to issues regarding health data such as interoperability, access control, data ownership and data provenance. However, challenges such as high-velocity clinical environments, health data security and authentications of health data have also been described as areas where the characteristics of blockchain might have a fit [100].

The first systematic review on the topic of blockchain in healthcare suggested that the exploration and implementation of blockchain technology in healthcare is on the rise. Trends at that time (2018) in blockchain research for healthcare primarily focused on data sharing, health records, and access control, but there was limited suggestion for other applications such as supply chain management or drug prescription management. The implications made from this were that there is a significant untapped potential for blockchain in healthcare [101]. The second systematic review (2019) reached similar conclusions that blockchain technology has potential to address some of the difficulties encountered by the healthcare sector. The most promising applications of blockchain technology in healthcare are well-researched areas, including security, integrity, decentralization, accessibility, and authentication principles, due to the underlying infrastructure of the general ledger and blocks. It is evident that blockchain offers numerous advantages that can be utilized to address various issues related to data sharing and security within the healthcare industry. However, it is important to note that blockchain is not a one-size-fits-all solution and its implementation should be thoroughly evaluated in relation to specific challenges within healthcare. Careful examination of how blockchain can address these challenges is necessary [102]. The research field was, in 2018, clouded by theoretical concepts that were far from reality. More systematic domain focused research was therefore needed. How blockchain could work in the context of virtual healthcare, learning health systems, and trust within the patient-physician interaction had also not been explored. In later reviews (2022), conclusion that incorporating blockchain technology into healthcare systems poses certain technical challenges, such as the immaturity of blockchain, scalability issues, lack of interoperability, standalone projects, difficulties in integrating with existing healthcare systems, complexity, and a shortage of professionals with blockchain expertise were made. These challenges must be addressed in order to effectively integrate blockchain into healthcare systems [103].

2.6 Rationale

As outlined previously, challenges around trust, access control, data transparency and data provenance are present in health information systems and e-health applications [32, 49]. Meanwhile, the emerging blockchain technology provides inherited characteristics that could provide data transparency, tamper-proofness, data integrity, and provenance [65]. Therefore, a logical research objective would be to explore if and how blockchain technology could provide any value to these challenges and the health system as a whole. Furthermore, the rationale in this research project also lies in the importance of systematical review and experiment with an emerging, decentralized technology that upon the start of this project was lacking in the academic literature, and it is crucial to proceed with a systematic research approach to a topic that in the middle of 2018 (the start of this project) consisted mainly of loose ideas and concepts, many of them far from reality and real-use cases [8]. Previous research have also expressed the challenges with blockchain being an immature technology and that more research is need to explore to potential of blockchain in the health domain [103]. As blockchain has been suggested to not be a one-size-fits-all solution in the health domain it is important to further explore the need for this technology and identifying real-world use cases where the technology potentially could provide value [102]. There are suggestion of where blockchain potentially could have a fit in this domain, but the current literature lacks further exploration on this topic [100]. With the theoretical foundation in the health science discipline and by applying design theory, using the best-practice methodology, this research project provides a systemic and scientific lens to the following research aim:

The aim of the research project is to explore the topic of blockchain applications in health information systems. Furthermore, the aim extends to designing and developing an e-health related service that utilizes the properties of blockchain and to evaluate that service.

2.7 Research objectives

Obtain a systematic overview of scientific literature that proposes blockchain technology, to improve processes and/or services in healthcare, health sciences and health education.

Propose a concept that has a technical infrastructure which is supported by blockchain technology, and that therefore enables an immutable record of patient-physician encounters in a virtual healthcare environment.

Evaluate a prototype of the developed service through using a group of medical students to assess the service's capacity as a telemedicine and educational tool.

2.7.1 Research questions

RQ1: What is the current state of knowledge on the topic of blockchain applications in the health domain?

RQ2: What are the potential problems in health information systems where blockchain could have a high fit-for-purpose?

RQ3: What are the perceptions of a decentralized competence verification system amongst medical students?

RQ4: How could PROMS work as a means of learning and improvements for healthcare professionals?

Table 2.3 provides an overview of which sub-study explores the research questions.

Table 2.3: Overview of research questions and papers

Research questions:	**Explored in:**
RQ1: What is the current state of knowledge on the topic of blockchain applications in the health domain?	**Paper A**
RQ2: What are the potential problems in health information systems where blockchain could have a high fit-for-purpose?	**Paper A** and **Paper B**
RQ3: What are the perceptions of a decentralized competence verification system amongst medical students?	**Paper C**
RQ4:How could PROMS work as a means of learning and improvements for healthcare professionals?	**Paper B** and **Paper C**

3 Research approach

As previously mentioned, this project is highly interdisciplinary and handles a new, emerging technology. Therefore, the project could be explored through different perspectives or academic lenses, such as ICT, cryptography, health informatics, or general technology development. This project has applied the lens from the development of health informatics technology. The scope of this project fits well within this field of research.

Health informatics is the research discipline that studies HIS and its components. Health informatics research is specially focused on [28]:

1. Understanding the fundamental nature of ICT processes and describing the principles shaping them.
2. Developing interventions that can improve upon existing ICT processes.
3. Developing methods and principles that allow such interventions to be designed.
4. Evaluating the impact of these interventions.

The overall framework of health informatics research has influenced this research project, items two and four in the above list being emphasized in particular. Two main approaches can be applied to the design and introduction of technology: a technology-driven approach, in which problems are solved through the use of a specific technology, or a problem-driven approach, which involves the solution of defined problems. These two approaches are the foundation on which the determination of which approach to adopt was based [28]. This research project has adopted the latter approach and relies on design science and user-centered design theory.

3.1 Design science

Health informatics research and informatics- and computer science research in general often have a research agenda to design and evaluate new artifacts. This has been referred to as "creation research strategy" [104], but is more commonly known as design science [105]. The artifacts in such research can be models, concepts, methods, or working systems, which can be used to various degrees to demonstrate models and concepts.

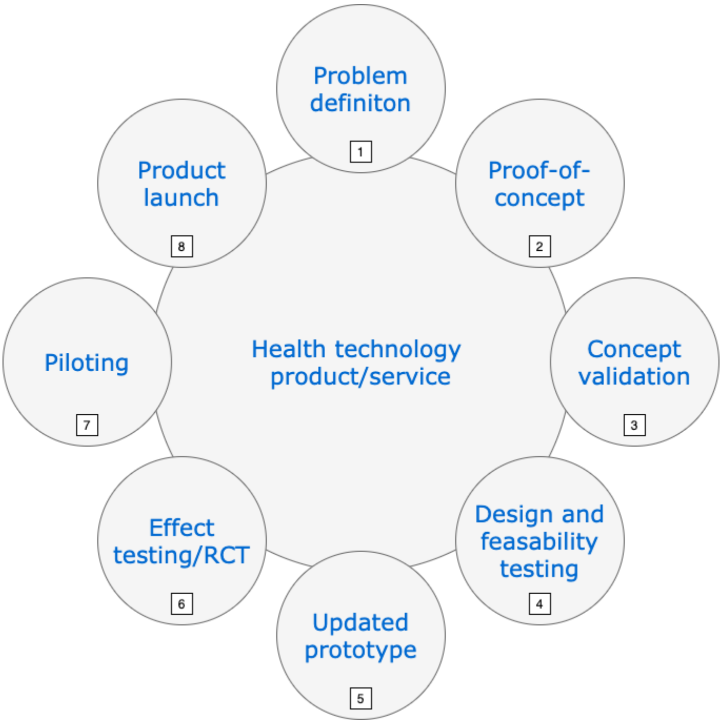


Figure 3.1: Development cycle for e-health applications

The engineering cycle is a common design science framework, which can be used to guide the developer/researcher through the different stages of development [106]. Figure 3.1 shows a cycle specifically developed for the design and development of medical technology, which was used in this project. The framework and figure were adopted from the development stages for medical devices outlined by the U.S food and drug administration (FDA) [107]. The development of medical technology is a complex and time-consuming endeavor. This project has, therefore, not completed the entire cycle of development, just phases one to four. Phase five is in progress. Previous research supports this approach, it being also emphasized that the established phases of development should be followed in the creation of artifacts through using design science [104]. There are other design frameworks, such as the double diamond design process [108] which with the none-linear phases of discover, define, develop and deliver aim to achieve the same goal as the engineering cycle. The engineering cycle was chosen over other frameworks based on its simplicity and clarity.

A qualitative case study approach was used to validate the concept (phase four), the qualitative approach providing artifact development with a holistic perspective [104]. A user-centered design approach was adopted in this stage.

3.2 User-centered design

User involvement can be considered to be a crucial element in any successful ICT development [109]. A user-centered design was therefore applied in the later stages of this research project. The term "user-centered design" was introduced by Donald Norman of the University of California San Diego in the 1980s with his work User-Centered System Design: New Perspectives on Human-Computer Interaction [110]. This introduced user-centered design, which became an accepted scientific theory in the design of products and services that involve a user.

Norman provides four basic suggestions on how a design should be undertaken, all placing the user at the center of the design process. These are widely accepted by the user-centered design community [111]:

1. Make it easy to determine what actions are possible at any moment.
2. Make things visible, including the conceptual model of the system, the alternative actions, and the results of actions.
3. Make it easy to evaluate the current state of the system.
4. Follow natural mappings between intentions and the required actions; between actions and the effect; and between the visible information and the interpretation of the system state.

The objective of user-centered design is to ensure that the product (or service, or interface) meets the user's needs. Involving end-users in the development process was therefore considered to be essential in this project. The users involved in the user-centered design process can play different roles, Druin distinguishing four different roles: user, tester, informant and design partner [112]. The user in this project had the role of a tester. This means that users were observed when testing a developed mock-up of a prototype. The development and testing of the mock-up followed Norman's suggestions, particularly item two in the above list; make things visible, including the conceptual model of the system, the alternative actions, and the results of actions.

4 Methods

The methodology of this project is anchored in the design science approach described in the previous section. The project began with problem definition as the first step, which was approached via a systematic review of the peer-reviewed literature in this field. Gaps in the research were, based on this review, identified and a problem in which blockchain might be able to provide value was defined through involving expert opinions and gained "know-how".

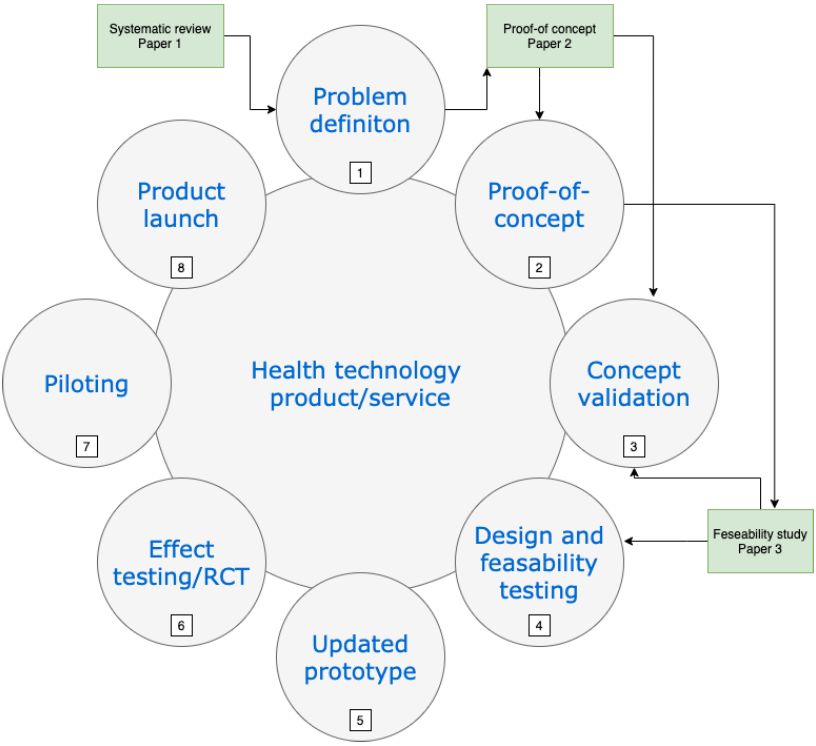


Figure 4.1: Research approach to the development cycle

The methods for each of the three separate studies are summarised in the following sub-sections. The methodology can also be read in full in **Paper A**, **Paper B** and **Paper C**.

4.1 Systematic literature review

A systematic literature review is a type of literature review that aims to comprehensively and systematically identify, evaluate, and synthesize all available research evidence on a specific research question and follows a predetermined and standardized process to search, screen, and select studies, assess their quality, and extract and synthesize data in a transparent and reproducible manner [113].

A structured literature search on the topic was conducted in accordance with the PRISMA statement [113]. A systematic search strategy was developed, which included searches in MEDLINE, Embase, Cochrane Library, Scopus, Google Scholar, Compendex, Inspec, ACM and IEEE, these capturing the interdisciplinary focus of the topic. A total of nine databases were searched and are inline with recommendations that more than one database should be searched for systematic reviews [114]. Embase, MEDLINE, Web of Science, and Google Scholar are recommended data bases as a minimum requirement for a systematic review in medical science [115]. The search was also applied to the Cochrane Library (Cochrane Database of Systematic Reviews (CDRS), the Cochrane Central Register of Controlled Trials (CENTRAL)), to identify other related systematic reviews. The databases Inspec [116], ACM [117] and IEEE [118] are the most widely used databases in the engineering field and were added to capture publications that may not have been indexed by the databases related to medical science. From Google Scholar the first 500 search results were included in the screening. A protocol was developed with defined inclusion and exclusion criteria. Both the search strategy and the protocol for the study are appendices to the digital version of **Paper A**. Titles, abstracts and full articles were subsequently screened by reviewer 1 [AH], through the application of the predetermined inclusion and exclusion criteria. Publications meeting the inclusive criteria, but which the first reviewer was in doubt about, were reviewed a second time by three additional reviewers [AF, KK and DG]. These publications were discussed by all four reviewers to determine whether they should be included or excluded. The screening process is given in 4.2.

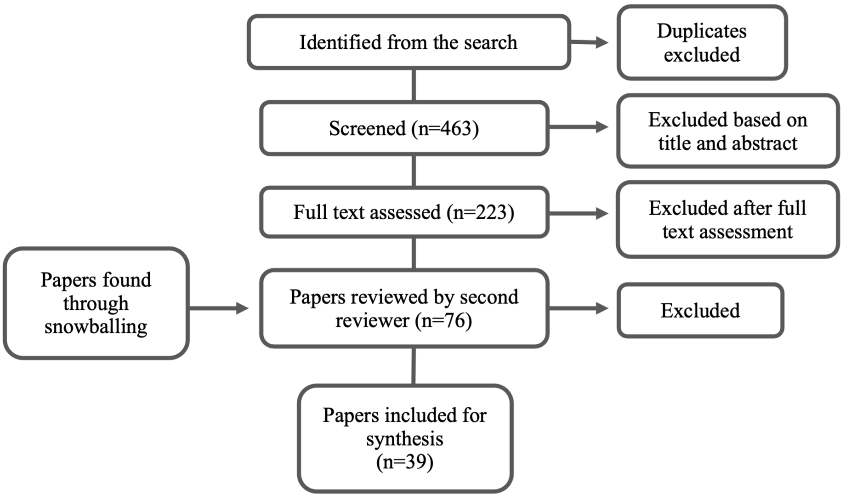


Figure 4.2: Inclusion flowchart [10, p. 4]

Data from the papers included in the review was extracted according to a pre-defined matrix, and reviewed by several authors to give increased objectivity. The quality of the publications was also considered [119]. A detailed quality assessment was therefore performed.

4.2 Proof-of-Concept

A proof of concept, is a crucial method for showcasing the capabilities and appropriateness of software for users and stakeholders and proving that the idea is viable and meets the needs. Proof-of-concepts can be applied in various fields, such as marketing and medicine, but in the context of software development, it refers to a specific process that can involve the development of hardware, websites, or other software to put a concept into practice. The purpose of this process is to determine whether a software idea can be realized, the technology that should be used for development, and if the intended users are likely to adopt the software [120]. The term proof-of-concept is used in the context of software development in this work.

The methodical framework proposed by Campbell et al. was adopted, modified and followed to address the second objective of this research project [121]. This is illustrated in Figure 4.3. The framework was initially used to design and evaluate complex interventions (interventions with several components) within healthcare. This study, however, addressed two critical issues outlined in the framework; (i) establishing the theoretical basis of the intervention and (ii) identifying and

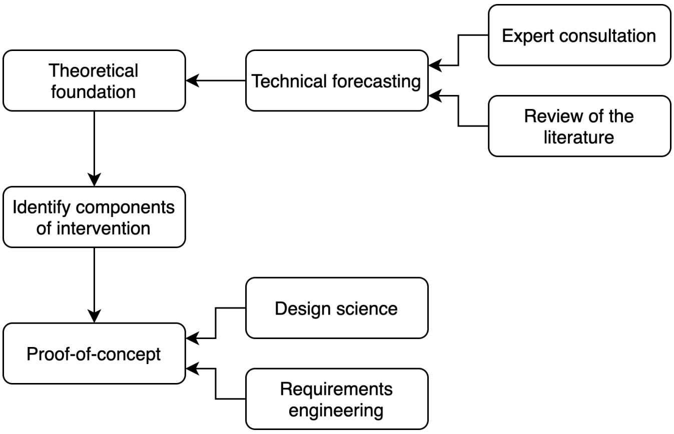


Figure 4.3: Research approach in study B [12, p. 4]

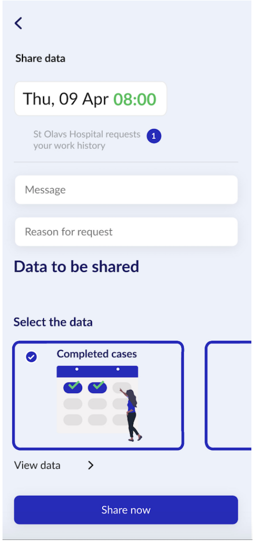
describing the components of the complex intervention. The interdisciplinary team, who possess a collective knowledge from both the technical and domain side, served as the expert input group. This team conducted the first validation of the requirements obtained from the requirements engineering process, and determined whether these corresponded to real-world problems and regulatory requirements. This validation was carried out through a number of joint workshops.

A proof-of-concept was developed using the principles of design science, as described previously [122] and requirement engineering. Requirement engineering is a process in which the requirements for the artifact under development are defined, and can include domain analysis, elicitation, specification, assessment, negotiation, documentation, and evolution [123]. Requirement engineering is generally accepted to be the most critical and complex process in the development of socio-technical systems [124]. The first requirement definition was based on the initial understanding of the problem, and on input from the first phase of the study. The requirements were then used to create an architectural model, the architecture being used to implement a proof-of-concept application, the primary artifact of the project. The next step in the engineering cycle determines whether the assumptions made were incorrect or whether the process reveals unexpected problems, the process goes back one step if this proves to be true.

The concept was named VerifyMed and will be referred to by that name in this thesis.

4.3 Feasibility study

A mock-up of the user interface of the VerifyMed service was developed to achieve the objectives of this sub-study. The mock-up can be accessed here [125]. Figure 4.4 provides an example of the user interface tested in this study.



Thu, 09 Apr 08:00

St Olavs Hospital requests your work history 1

Figure 4.4: Example page of the user-interface

The interactive prototype was evaluated from the perspective of the users (medical students) using usability testing [126]. A qualitative research method was considered to be the most appropriate method for answering the research questions [127, 128]. An user-based evaluation which is an usability evaluation method where users directly participate in the testing. In such test, users usually get some tasks to perform with a product or a service and their behaviour, errors and difficulties are observed [129]. These steps were adopted according to best practice: test objectives were defined, recruitment of tests participants, creation and description of the task scenarios, definition of measurement and data that will be collected, preparation of the test materials and of the test environment, choice of the tester, selection of satisfactory questionnaires, the data analyses procedures, and presentation and communication of the test results [129].

Data was collected through conducting nine semi-structured interviews, the System Usability Scale (SUS) being used [130] as a starting point for the interviews. Two focus groups, one of four and one of five participants, were run. The recruitment of participants was ended when it was concluded that the data had reached saturation [131].

Data from the interviews and the focus groups were transcribed according to the six steps of transcription proposed by Azeyodo et al. [132]. The data, after being transcribed and translated into English, was analyzed according to the principles of systematic text condensation [133], the procedure consisting of four steps: (1) gaining a total impression by reading all the text materials and identifying preliminary themes, (2) identifying meaningful units from both the technical aspects of the VerifyMed service and its use by medical students, (3) abstracting condensates from each group and subgroup, and (4) creating synthesized descriptions of user experiences and opinions on the use of a decentralized work history portfolio.

4.4 Ethical considerations

Human participants were only included in the third study of this research project - the feasibility study. No ethical issues or considerations were therefore identified in the other studies. The following considerations were applied to the feasibility study: All participants were asked to give a written consent based on oral and written information about the study. According to the consent form, only those who consent to participate in the study were included (n=9). The study did not collect or otherwise handled patient or health-related data. Therefore, ethical clearance from the Regional Ethical Committee (REK) was not obtained. The study was registered by NSD - Norwegian Center for Research Data and the Data Protection Officer at the Faculty of Medicine and Health Science (Norwegian University of Science and Technology) to be General Data Protection Regulation compliant [12].

5 Main contributions

A summary of the findings of the three studies (**Paper A**, **B** and **C**) are presented in the following sections. The figures and tables presented here were first published in their respective paper, and the overall findings and the coherence of the three studies are discussed in the next chapter (Discussion).

5.1 State-of-Knowledge

As Figure 4.2 shows 39 of the 463 publications were included in the review.

The publications included in the review describe a number of systems, processes and challenges in the health domain, in which it was suggested that blockchain enhanced concepts could form part of the solution. The most frequently described system was EHR (Table 5.1), 43% of the publications referring to this system. Other systems referred to were PHR (15%) and clinical trial support systems (5%). The target system processes primarily focused on the sharing, storage, exchange and access of medical data, more than half of the publications (62%) referring to processes that share health data. Many of the PHRs were proposed as patient-controlled, and were not tethered to a particular health institution or system.

Table 5.1: Bibliographic overview [10, p. 7]

Information system category	Count	Proportion
Electronic health records	17	43 %
Personal health records	6	15 %
Clinical Trial Support Systems	2	5 %
Knowledge infrastructures	1	3 %
Picture archiving and communications systems	1	3 %
IoT data management/Personal health data	1	3 %
Automated diagnostic service for patients	1	3 %
Administrative systems	1	3 %
Electronic health records/Administrative system	1	3 %
Population health management system	1	3 %
Pharma supply-chain	1	3 %
Grand Total	39	

Figure 5.1 shows that the consortium blockchain (38%) was the most used blockchain type in the publications. A number of the papers did, however, not define the approach (26%). Private (10%) and public blockchains (15%) however appear to be less used in the health domain. Ethereum was used in eleven (28%) of the 39 publications included in the review, Hyperledger Fabric four times (10%) and Exonum once (4%). Eight (21%) of the studies did not specify a platform or framework. Fourteen studies (36%) in the review appear to have developed a new blockchain for their concepts.

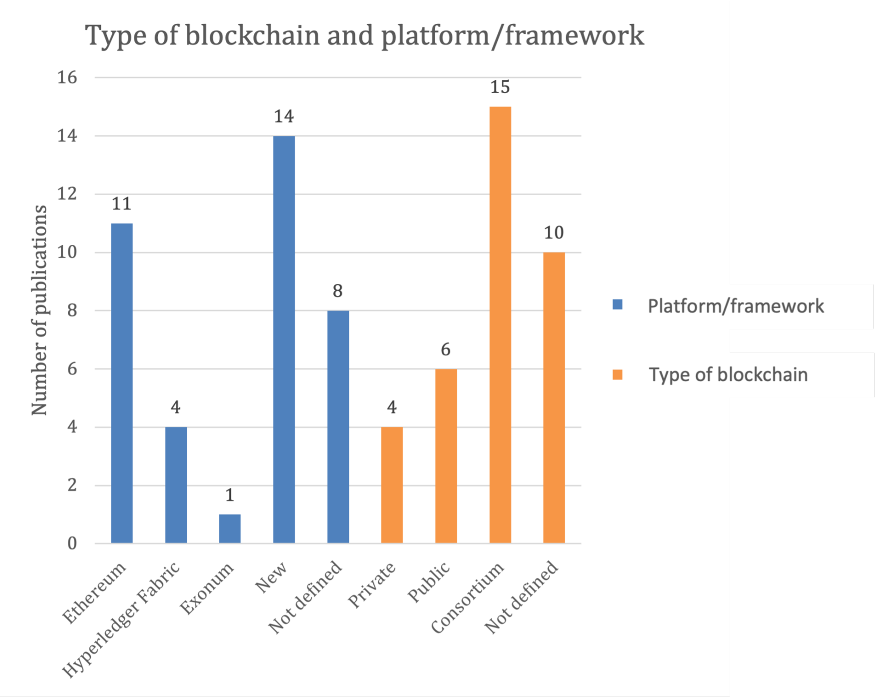


Figure 5.1: Type of blockchain and platform [10, p. 7]

The results show that a variety of consensus algorithms have been used in healthcare (Table 5.2). The most frequently used consensus algorithm in the publications included in the review was PoW (21%). The second most frequently used consensus algorithm was PBTF (15%). It should be noted that not all concepts built using the Ethereum platform or Ethereum protocols used PoW. A number of publications (41%) did not state the consensus protocol their concept would apply. Smart-contracts were a feature in several of the proposed concepts, 38% of the studies using smart contracts for some functionality. The remaining studies in the review did not define whether smart-contracts were a feature or not (Table 5.2).

Table 5.2: Consensus algorithms and the use of smart-contracts [10, p. 7]

Consensus algorithm	**Count**
Proof of Work (PoW)	8
Proof of Work (by pre-selected miner)	1
Practical Byzantine Fault Tolerance (PBFT)	6
Proof of Stake (PoS)	1
Proof of Interoperability	1
Proof of Conformance	1
Permissioned Voting-based	2
Ledger-based Byzantine Fault Tolerance	1
Hybrid (Delegated PoS + PBFT)	1
QuorumChain consensus	1
Not defined	16
Use of smart contracts	
Yes	15
Not defined	24

The systematic review results indicate a small number of main challenges that the blockchain concept attempted to address: access control, interoperability, provenance verification, and data integrity.

The results did not show any blockchain solutions for medical educational proposes, healthcare professional credentials, or trust in virtual healthcare.

5.2 Proof-of-Concept

The proof-of-concept of VerifyMed and its architecture are described in this section.

A proof-of-concept was developed based on an identified need. This need was identified based on the results of **Paper A** and the research of the second study of this project. The need can be summarized as follows: perceived competence and perceived goodwill are contributing factors to system and interpersonal trust [51, 60]. It also becomes increasingly important in a virtualized health care environment to verify the competence and credentials of health care professionals, to establish and maintain trust within the interaction [134].

The architecture was designed to enhance trust. This was achieved by introducing three items of healthcare professional evidence to prove competence and verification: evidence of authorization, evidence of experience, and evidence of competence [135]. The architecture also includes tools for evaluating these interactions publicly on the blockchain.

General principles for requirements and system design have been defined in previous research on blockchain applications, within the healthcare industry. These are suggested followed and have been adopted in this work [97]. The principles and metrics for evaluating blockchain applications within the healthcare industry are primarily tailored to the American Health Insurance Portability and Accountability Act (HIPAA). These were, however, modified and generalized in this work. An architectural framework was designed based on functional and non-functional requirements, non-functional requirements describing system properties such as security, privacy, and performance requirements. These have a sizable architectural impact on the system. Functional requirements present the functionality which is required within the architecture, these being further described in **Paper B**.

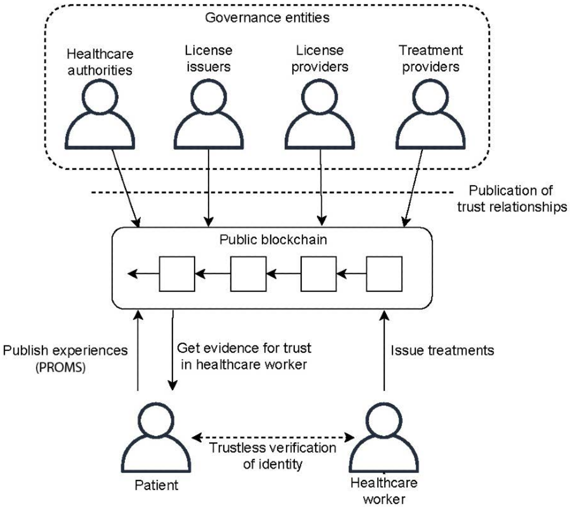


Figure 5.2: The VerifyMed architecture [11, p. 9]

5.3 Feasibility study

The study included a total of nine participants. They were all individually interviewed and all participated in one of the focus groups. A summary of the participants is presented in Table 5.3.

Table 5.3: Characteristics of the informants (n=9) [12, p. 5]

Characteristics	Value
Gender	**n (%)**
Men	4 (44)
Women	5 (56)
Age	**n (%)**
23 - 24	3 (33)
25 - 26	2 (22)
27 - 28	3 (33)
<28	1 (11)
Study year (of six)	**n (%)**
4	1 (11)
5	5 (56)
6	3 (33)
University	**n (%)**
Norwegian University of Science and Technology	8 (89)
University of Oslo	1 (11)
Previous knowledge of blockchain	**n (%)**
No	6 (67)
Yes	3 (33)

Note. Percentage is rounded to nearest integer

The SUS questionnaire was used as a starting point for the interviews, as described in the method section. The primary objective was not to collect quantitative data. Quantitative results were, however, calculated using the standard formula for SUS [136]. The score was 69.7, responses being fairly equal across respondents. The average SUS score in general is 67, 70 being considered by validation studies to be a good score [136].

Five themes were identified by the data analysis of the interview and focus group data. A summary of this is presented in Table 5.4. The results from the interviews and from the focus group were intertwined, the same themes being discussed in both and therefore presented jointly.

A more detailed and in-depth presentation of the feasibility study findings is given in **Paper C**. A couple of significant findings are presented here, to help the reader gain an overall understanding of the coherence of the PhD project. The reader is, however, advised to read the whole study.

The data from the individual interviews shows that there is a need for digital verification, and that this could be particularly important in a virtual healthcare environment.

"Showcasing courses and similar could contribute - it becomes the same as having diplomas on the wall. Whether a patient understands what these are is uncertain, but it can increase the overall impression."

Some participants displayed a hesitancy in accepting this, and were uncertain how patients would interpret the information.

"...I'm a bit uncertain about this. What value could they being able to see this bring. It might be difficult for them to interpret it. It's difficult to say what they would use this information for."

The last main theme discussed was the VerifyMed user design and features that all respondents were exposed to, and suggestions for general improvements and opinions of the system. None of the respondents had any problems completing the nine-item task list, doing so within a short space of time (3-7 min). The general expression was that the solution could be useful. The need for this kind of service was acknowledged. One respondent expressed this as follows:

"I envision a future in which things are more digital, that patients who have a specific problem want to contact a doctor who has researched or has courses within that area. It could be very useful for a doctor to be able to show their knowledge and interests in that area. More patients might then be willing to be included in their research and you may get more patients that you find interesting."

The informants expressed that they were familiar and comfortable with the design and user-flow. They had a few suggestions for improvements, including the addition of features such as: (1) Make it clearer what data is being shared, for how long, and with whom; (2) Make direct communication with patients possible through a message system; (3) Make showcasing scientific publications or research projects possible as a part of the "portfolio."

Table 5.4: Results overview [12, p. 5]

Theme	Proportion of the data	Supporting quote
The need for aggregated storage of work- and study-related verifications	24,2%	"...large parts of the system is trust-based. I don´t know how to verify certificates, but as you say, paper-based certificates are an easy way to falsify knowledge and experience."
Trust in a virtual healthcare environment	26%	"To showcase what you have done related to courses and such could contribute, it becomes the equivalent to have diplomas on the wall. It is not necessarily certain that the patient understands what it is, but it can improve the total impression"
The potential use of patient feedback	14,5%	"The ones who write feedback are the patients how are either very pleased or they who are very displeased. ...the selection gets skewed."
Trust in blockchain technology	7,3%	"I think I understand the value with that things could be verified and that falsification might be mitigated with time-stamping and such, that I see as positive..."
Improvements of the VerifyMed concept	6,5 %	"I envision that in the future when things get more digital and patients have a specific problem and want to get in contact with a doctor who has done research in that area or has any specific courses within the area..."
Note. The Percentages do not add to a 100 since other themes not relevant to the research questions also were discussed		

6 Discussion

The aim of this research was to explore blockchain in health information systems, this aim extending to the design and development of an e-health service that utilizes the properties of blockchain, and the evaluation of this service. Three separate studies were carried out to realize this aim. They were presented earlier in this thesis, the papers themselves also being attached here. Their combined findings, limitations and related considerations are discussed in this section.

No systematic literature reviews had been published on "Blockchain in healthcare" at the point of time that the research protocol for the literature review was developed. Two review papers were published on this topic before the publication of **Paper A**. The systematic review prepared in this research presents a valuable summary of the literature published up to the point in time of the review that supplements the other reviews published on the topic. The findings provide an extensive overview of the areas in health systems targeted by blockchain solutions. This overview also summarizes technical specifications, and the quality of the research undertaken in the academic (peer-reviewed) setting. The findings show that the reviewed publications in general lacked more technical detail, which may be the cause of a gap between concepts and implementation. The overview also shows too many research projects not moving past the concept stage. How this new technology can function in the health domain therefore needs to be further explored, to move the technology forward. Feasibility assessments should also be conducted to find high fit-for-purpose solutions and new research should address blockchain-based solution compliance with current health data laws and standards. Real-world implementation feasibility should furthermore be increased, by exploring which blockchain features and designs comply with these data and privacy laws and regulations.

The results from **Paper 2** indicate that there are a number of areas in which GDPR and blockchain are in conflict. Discussions around this in the blockchain research community and amongst policymakers are therefore necessary to make GDPR (and other regulatory frameworks) a protector of privacy and security, and not a factor that hinders blockchain innovation.

The results of the second study (**Paper B**) allowed the definition of the hypothesis, this being that trust requirements such as (1) the caregiver must trust that the patient exists, (2) the caregiver must trust the authenticity of the data that the patient is willing to share, and (3) a third party (e.g., an insurance company) must be able to trust the patient's claim that care provision has taken place, and that these requirements have the capacity to enhance general trust in the patient-physician interaction in a virtual healthcare environment. The following theoretical challenges to trust, in a virtual healthcare environment, were formulated as a basis for the development of the concept. This is described further in **Paper B**. The patient needs to trust that the caregiver has the right competence (and authorization) to deal with his or her health problem in both a physical and in a virtualized health care environment. The caregiver needs to show the patient that he or she possesses the competence required to deal with their health problem. The patient is likely to otherwise go somewhere else. A potential risk in the concept is that the patient is not able to understand the credentials and experience of a caregiver. Having a license is not the same as having credentials, and having competency is not the same as having experience. The system should therefore make the patient's credentials or competency contextually meaningful.

The trust mechanism enabled by blockchain in VerifyMed provides a transparent, accountable, and controlled means of handling the verification of competence and experience. This could, however, also possibly be achieved by a centralized solution. The main advantage of a blockchain solution is decentralization, the importance of which may increase as the healthcare industry transforms to a digital-driven domain. It is important to compare blockchain solutions with more conventional technologies, an aspect which should be further explored in new research.

The very high levels of energy consumed by blockchain, due to the computational power required by PoW, is a central argument against its use [137]. This is a significant issue for cryptocurrencies such as Bitcoin which use PoW. Ethereum used PoW up until the end of 2022 and has nowed moved to PoS in Ethereum 2.0. This level of energy consumption makes transactions expensive and arguably makes the system climate unfriendly. This problem is, however, more nuanced then this. The source of the electricity used in PoW is a crucial aspect. For example, arguments in favor of PoW are based on that PoW can use excess electricity in the grid, and can use clean electricity from renewable sources. Other suppliers of both currency and stores of value such as gold also consume energy. **Paper A** showed that a very few developed solutions in the health domains that are based on blockchain, used PoW, which is the consensus mechanism that makes most sense in a public blockchain. The majority of advanced concepts, however, used either private or consortium blockchains. Ethereum was used for the PoC in VerifyMed, this choice being based on the ease of development in Solidity (the Ethereum programming language) and the large community of developers who work on Ethereum and Solidity. The results of the PoC study show that the cost of transactions in systems that use PoC would be very high, and even higher today after the increases in price of Ether (the cryptocurrencies of Ethereum) that have taken place since PoC was developed (**Paper 1**). An updated version of VerifyMed will use another consensus mechanism. Transactions will therefore become cheaper and possibly more eco-friendly.

The feasibility study (**Paper C**) validated the need for the VerifyMed concept, the study clearly establishing that the solution fills a need defined by the user group exposed to the concept. Some of the feedback from users indicates that minor modifications should be made to the concept, including: putting the user in more control of the data sharing function, the provision of reputation control, and an objective feedback system. This input will be taken forward to the next phase of the development cycle, phase four (Figure 3.1). The users were also optimistic about utilizing PROMs as a learning mechanism in their professional development. They rarely received information on the outcomes of the care they provided, especially when working in a virtual environment. They saw this as a way to learn from mistakes and to promote successful intervention. PROMs are incorporated into VerifyMed, to validate the experience of healthcare professionals and as a learning mechanism. This, however, requires a high proportion of patients to take the time to submit answers to PROM surveys. A cryptographic protocol was created to incentivize patients, and to increase participation rates, the protocol rewarding a patient with a digital token, which can be exchanged for new health services. **Paper 5** provides a complete presentation of this solution, which will be built into an updated version of VerifyMed as a feature. The use of PROMs as a learning health professional mechanism could contribute (at a higher level) to the concept of the learning health system.

Following the development cycle enhances the development of a high-quality and fit-for-purpose system. One conclusion that can be drawn from the feasibility study is that a decentralized system for storage of work-related verifiable credentials could increase trust in the health system. This is particularly true where there are fewer trusted institutions, due to an increase in the number of health care providers in a digitally transformed healthcare system.

Previous research has indicated that there was a lack of blockchain research projects outside the use-cases of data sharing, health records, and access control within the health domain [101]. This research project has targeted a use-case where blockchain so far has not been proposed as a technology that could provide value. This novel approach makes a contribution and extents the overall knowledge within the field. As previous research has suggested that blockchain is not a one-size-fits-all solution and its usage needs to be properly evaluated to specific challenges and use-cases [102]. This research project has therefore used methods of design engineering to find the right use-case and modify the technology there after. For example, the first version of VerifyMed was built on an open public blockchain (Ethereum), through experiments in the proof of concept study (**Paper 2**) it was concluded that the use of Ethereum become so expensive that the application was infeasible for real-world use. This knowledge was taken into consideration when the new version of VerifyMed was designed. These results and approach are an evidence that what previous research has suggested of no one-size-fits-all solution seems to be correct.

State-of-the-art research has also suggested other challenges for using blockchain in healthcare, such as the immaturity of blockchain, scalability issues, lack of interoperability, standalone projects, difficulties in integrating with existing healthcare systems, complexity, and a shortage of professionals with blockchain expertise [103]. This project also showed the scalability issues when using a public blockchain. This could probably be improved by using permissioned blockchains instead, due to the lower monetary cost of running them. This research project has not been able to show a solution that can overcome the other challenges mentioned here. With that said, the field is growing and so does the professionals with this kind of expertise. So the fact that research has been done, which this project contributes to, the knowledge and the number of people who obtain this knowledge increases. This project has not been able to show an integration towards existing systems, but this will be on the research agenda for the contingency of this project.

6.1 Significance of the contributions

It is essential to systematically explore the new technologies brought by the digital transformation, and their potential impact on health systems. HIS will continue to be a core building block in maintaining the key functions of a health system in the current digital transformation (improve health, legitimate responsiveness to population expectations and fairness in financial contribution), a role that is likely to become increasingly more important. This research has explored the relevance of blockchain in HIS, by systematically following a design science approach.

This research work includes three separate studies. The first contribution is being one of the first systematic reviews of the current state-of-art and state-of-knowledge under this topic (**Paper A**). This study makes a significant contribution to the field by systematically summarizing the research being done by the time of the review. This study was the third systematic review published on the topic, with the two first studies published shortly before. The importance of this study can be confirmed by the high number of citations it has. The second contribution, a novel problem which blockchain could potentially impact, was defined based on the results of this study and the first objective of the second study (**Paper B**). A proof-of-concept was developed, following the principles of requirement engineering. As an outcome of the systematic review, it was concluded that a lot of research being done in the topic did not have a systematic and scientific approach. (**Paper B**) aimed to improve that by adopting methods commonly used in medical research. As a result, this study shows that a blockchain solution for a specific, systematically well-considered use-case in the health domain is technically feasible. The last contribution is exposing end-users to the proof-of-concept, to provide early validation and user input, this following the theory of user-centered design (**Paper C**). This study is one of a few where the technology of blockchain is being exposed to the users within the health domain and by that, making a significant contribution to the topic. The combined strengths in these three separate studies are that they build upon each other according to the theory of applied engineering [106]. Continuing the applied engineering cycle is likely to yield more exciting research opportunities.

An advantage of this research project is the interdisciplinary approach applied to the multi-leveled topic of blockchain in HIS. It is important to properly explore the use of this new technology in health systems, to fully comprehend the technology, the opportunities it provides and the impact of different design choices on fit-for-purpose. It is also equally important to maintain a domain focus, to define challenges in which the technology might fit, to obtain input from end-users and validate the exploration using sound and accepted scientific methods from health science. This is particularly important in this topic, as a great deal of unrealistic, unfeasible and underdeveloped concepts circulate in the literature [10].

This project falls under the umbrella of digital transformation research. It is therefore of interest to evaluate how blockchain fits within digital transformation. Digital transformation has four dimensions, which apply irrespective of industry; use of technologies, changes in value creation, structural changes, and financial aspects. This work primarily addresses the first dimension, the use of technologies. Blockchain could, however, also address the other dimensions in health systems, and could provide new methods of value creation, a new decentralized structure for governance and consensus, and also financial aspects where cryptocurrencies or decentralized financing (Defi) are utilized. This should be considered in the future exploration of blockchain, for the digital transformation of health systems.

The COVID-19 pandemic seems to have expanded some components of the digital transformation in healthcare, telemedicine, in particular, being one of these components. Blockchain received a lot of attention during the COVID-19 pandemic, and was proposed (and used) in use-cases such as vaccination certificates [138] and contact tracing applications. Contact-tracing applications were a use-case in which blockchain was proposed at an early stage to increase data privacy. A mini-review/viewpoint paper (**Paper 3**), however, concluded that blockchain did not seem to contribute any value to these applications at the time of the review.

The philosophic position of this research work was based in positivism and with roots from evidence-based medicines, which entails that an objective truth exists and can be measured with scientific methods. This heavily domain focused research approach seems to be the most common approach in "traditional" health informatics research. The research work has maintained this perspective throughout the project, which has not been the case in the published literature under this topic. Most research projects seem to have a more technical focus and not that from a domain side. The insights and knowledge gained in this project are therefore unique, and contribute to the overall understanding of the value that blockchain can provide in the health domain.

6.2 Methodical considerations

Two developing technology directions for HIS can be taken, the technology-driven approach and problem-driven approach. This project, however, focused on a problem-driven approach. The project's main objective was previously set as part of the larger blockchain digital transformation initiative at NTNU, and had therefore been assigned a technology and a domain, but not a problem. This is the very definition of a technology-driven approach, and was therefore the default in the project. It was clear from the results of **Paper A** that many concepts and solutions in the health domain that use blockchain, did not have high fit for purpose. They were alternatively unable to describe this. This led to the conclusion that a problem-driven approach would be a better way of targeting the topic. Appraising the project from start to end shows that the two approaches have been applied and partially intertwined. The problem-driven approach was, however, the most prominent of the two. The engineering cycle adopted in this project has been shown to work well up to this point in time. This provides some validation that this has been a successful approach. A deeper evaluation should be carried out once the cycle is complete. The results, however, show that other researchers targeting similar objectives should adopt this engineering cycle (Figure 3.1) in their research.

In Paper A the term scoping review was used. However, the term systematic review which is a type of literature review that aims to comprehensively and systematically identify, evaluate, and synthesize all available research evidence on a specific research question and follows a predetermined and standardized process to search, screen, and select studies, assess their quality, and extract and synthesize data in a transparent and reproducible manner, would have been more descriptive of the study design [113]. As a scoping review is a type of literature review that aims to map and assess the scope, range, and distribution of research on a particular topic and it is typically used to identify the extent, nature, and characteristics of the available research evidence, as well as to identify gaps and areas for further research. Unlike systematic reviews, scoping reviews do not have predetermined inclusion and exclusion criteria and do not assess the quality of the studies. They are often used to provide an overview of a broad and diverse research landscape and inform future research design [139].

According to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, systematic reviews should be distinguished from scoping reviews based on their objectives, methods, and reporting. Systematic reviews should aim to answer a specific research question, use explicit and transparent methods to search, select, and synthesize studies, and report on the included studies' quality and risk of bias. Scoping reviews should aim to map the research on a specific topic, use flexible and inclusive methods to search, select, and synthesize studies, and report on the characteristics and distribution of the included studies [113].

With this knowledge, in **Paper A** the term systematic review should have been applied in the paper as the method used predetermined inclusion and exclusion criteria and systematically assessed the quality of the included studies.

A systematic literature review was chosen as the method to fulfill the objective of the study - systematically review, assess and synthesize peer-reviewed publications utilizing/proposing to utilize blockchain to improve processes and services in healthcare, health sciences and health education. Another method to review and assess the development in this field would have been to conduct and survey study by questioning experts in the field about the current development. However, this method was not used due to the difficulty of identifying experts at that point in time (there were many self-proclaimed experts) and lack of published systematic literature reviews at the time of the study design. The limitations of the systematic literature review approach is further described under limitations.

In the second study **Paper B** a Proof-of-concept was developed based on system requirements engineering. These requirements were formulated through the collection of expert opinions from informal discussions and workshops within the research group. This can also be described as a result of the forecasting analysis. Experts were consulted based on a convenience sample, and not on a comprehensive review of a larger group of experts. It is therefore impossible to conclude that this sample was not biased. A review of the literature, however, supports the input from the expert consulting. The review of the literature was in

Paper B defined as a scoping review. As previously mentioned, the term scoping review have many definitions [139] and by the time of publication of **Paper B** the reasoning was that the review work would fall under the definition of a scoping review. But by adopting this definition of scoping review (as previously) the review in the second study clearly falls out if this scope: "A scoping review or scoping study is a form of knowledge synthesis that addresses an exploratory research question aimed at mapping key concepts, types of evidence, and gaps in research related to a defined area or field by systematically searching, selecting, and synthesizing existing knowledge." [139, p.1292]. As the work review work done in **Paper B** did not systematically search, select and synthesized existing knowledge the conclusion is that the term unstructured literature review should have been used. This should be considered when reading however **Paper B** but should not affect the overall results and conclusions from the study.

In the second study, a proof-of-concept was chosen as an appropriate method to explore the capabilities and appropriateness of the concept. The proof-of-concept explores the technical feasibility of the concept. Another approach would have been to explore the user feasibility first, i.e. **Paper C** to make sure that the use-case and use of the technology would be worth further exploring. It was concluded to add a form of validation of the use-case and concept in the proof-of-concept study by collecting requirements from experts and reviewing the literature. Also, this work relied on the theoretical approach of the engineering cycle which indicates that a proof-of-concept comes before user feasibility [106]. Although, to proceed with the user feasibility study first would have been a less risky approach (mitigate risk of developing something that there is no need for) and it is probably preferred in future projects of similar character.

The third paper used a feasibility study to explore user perceptions of the concept and usability of the developed system. A more extensive study that includes quantifiable data such as a randomized controlled trial, could have given more generalizable results. It was however concluded that starting with a smaller feasibility study to gain early user feedback and validation, was the best first step. A qualitative feasibility study gives access to data quickly, which can be used to validate and improve the concept before designing any larger, qualitative studies. Therefore, a qualitative study was choice as the study design over a quantitative. For the evaluation of the usability of the system, a user-based evaluation was chosen as the appropriate method. The are three standard approaches for evaluating user interfaces: Model-, Inspection-, and User-Based Evaluations [129]. Model-based evaluation is considered as an immature and costly method, it was therefore excluded from consideration [140]. As the inspection-based evaluations do not involve the end-user but peer experts, the conclusion was that the value of presenting and validating both the concept and the interface to real users was preferred at this stage of the research.

The next step for the VerifyMed project, after the updates based on the results of the feasibility study have been made, would be to test the technology in a more extensive study and obtain quantitative data. This approach is in line with the development cycle used in the project (Figure 3.1).

6.3 Limitations

All research should consider its limitations, and this project is no exception.

A limitation of the systemic literature review was that it only captured development in the academic sphere. It did not include grey literature such as development by start-ups, large companies and governments. This might have led to an important development only found in the grey literature. But as private companies do not tend to publish their development results in open forums for commercial competitive reasons, it was difficult to capture this development in an academic review. However, a separate review on the same topic should explore the grey literature in future research.

There were also some limitations in the screening process in the literature review in **Paper A**. Ideally the screening process should have been done independently by at least two researchers to increase objectivity. In this case, the first screening process, based on title and abstract was done by one researcher. In the protocol for the study, clear inclusion- and exclusion criteria were developed. However, they were not validated through a test-screening before applied to the search result, which is also considered a limitation. As an implication of these two limitations, there is a risk that relevant publications were not included in the review. However, at the time of the search for the review, there were a few studies published on the topic, which is also confirmed by two other systematic reviews published prior to this one [101, 141]. These two studies had included a similar amount of papers, which could indicate that the screening process did work as intended. Nevertheless, the result of the study should be interpreted with these limitations in mind.

A framework for designing and evaluating complex interventions in health care was adopted in the second study, in a slightly modified form. The research approach and method of this study could have been based solely on design science and requirements engineering. There were, however, no real drawbacks of using the chosen framework.

The generalizability of the third study can be questioned, as it can for all qualitative research. Generalized results from case studies and other qualitative methods can be problematic [127], which is also true for this research project in which a technology is explored using a small participant group. General conclusions from the results should therefore be drawn with care. The project relies, however, on best-practice theory, and follows well-established research methods. It provides new insights that can add a small piece to the large puzzle of knowledge in this topic. Another drawback of this study is that it is limited to only one user-group. There are two major user-groups of VerifyMed, healthcare professionals and patients, and the feasibility study of this project included only the healthcare professionals. Testing with patients as users was not feasible due to the scope of this research project and COVID-19 pandemic restrictions.

6.4 Future research directions

The VerifyMed work should progress, from this research project, to the next phase in the development cycle. This includes developing an updated prototype based on the input from the feasibility study, and testing the effect with real users. An updated prototype should incorporate changes from the input given in **Paper C**, use an identity management system (explored in **Paper 4**) and use a blockchain with lower transaction fees (Ethereum used in the first version has relatively high transaction fees, explored in **Paper 1**). An updated prototype would allow a more extensive pilot study to be performed. It would also allow the collection of quantitative data that could target research objectives such as to explore the effect on patient trust of implementing transparent verification mechanisms for competence validation of physicians.

Blockchain is under constant development and new platforms, frameworks and use-cases are rapidly emerging. There are therefore new platforms to consider such as Avalanche [77], Cardano [142] and Solana [143]. New versions of VerifyMed should explore the possibility of moving the application to one of these blockchains. This could give lower transactions fees, higher throughput and an attractive development environment.

The ability to identify users is a crucial element of VerifyMed. There are a number of ways of achieving this. In Norway, the national widely used BankID solution could be utilized. A decentralized identity should, however, be implemented to truly achieve a decentralized user-centric solution. Some scoping work has been carried out under this topic (**Paper 4**), to explore the types of decentralized identity frameworks that could be utilized in VerifyMed. This should be further explored in an updated version of the concept.

The compliance of e-health solutions within the current regulatory and legal framework in the health system, is crucial for their ability to function in these systems. The compliance of VerifyMed with GDPR was explored in a separate study (**Paper 2**). Conclusions from this study show that there are a number of GDPR areas which blockchain struggles to comply with. This is an issue for all blockchain solutions. In the health domain, and for VerifyMed, further explorations need to investigate the compliance with other regulatory frameworks such as HIPAA and national health data laws.

Bibliography

[1] *NTNU digital transformation*. URL: `https://www.ntnu.edu/digital-transformation`.

[2] Department of Economic United Nations and Population Division Social Affairs. *World Population Prospects 2019: Volume I: Comprehensive Tables*. 2019.

[3] Rosie Ferris et al. “Perspectives of patients, clinicians, and health system leaders on changes needed to improve the health care and outcomes of older adults with multiple chronic conditions”. In: *Journal of aging and health* 30.5 (2018), pp. 778–799.

[4] European Commission Directorate-General for Economic and Financial Affairs. “The 2018 Ageing Report Economic and Budgetary Projections for the EU Member States (2016-2070)”. In: *Publication Office of the European Union* (2018).

[5] Christopher JL Murray and Julio Frenk. “A framework for assessing the performance of health systems”. In: *Bulletin of the world Health Organization* 78 (2000), pp. 717–731.

[6] Ritu Agarwal et al. “Research commentary—The digital transformation of healthcare: Current status and the road ahead”. In: *Information systems research* 21.4 (2010), pp. 796–809.

[7] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: 2021-09-22. Dec. 2008. URL: `https://bitcoin.org/bitcoin.pdf`.

[8] Matthias Mettler. “Blockchain technology in healthcare: The revolution starts here”. In: *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*. IEEE. 2016, pp. 1–3.

[9] Trisha Greenhalgh et al. “Tensions and paradoxes in electronic patient record research: a systematic literature review using the meta-narrative method”. In: *The Milbank Quarterly* 87.4 (2009), pp. 729–788.

[10] Anton Hasselgren et al. “Blockchain in healthcare and health sciences—A scoping review”. In: *International Journal of Medical Informatics* 134 (2020), p. 104040.

[11] Anton Hasselgren et al. “Blockchain for increased trust in virtual health care: proof-of-concept study”. In: *Journal of Medical Internet Research* 23.7 (2021), e28496.

[12] Anton Hasselgren et al. “Medical Students’ Perceptions of a Blockchain-Based Decentralized Work History and Credentials Portfolio: Qualitative Feasibility Study”. In: *JMIR Formative Research* 5.10 (2021), e33113.

[13] Ann Majchrzak, M Lynne Markus and Jonathan Wareham. “Designing for digital transformation”. In: *MIS quarterly* 40.2 (2016), pp. 267–278.

[14] Emily Henriette, Mondher Feki and Imed Boughzala. “The shape of digital transformation: a systematic literature review”. In: *MCIS 2015 proceedings* 10 (2015), pp. 431–443.

[15] R Scott Evans. “Electronic health records: then, now, and in the future”. In: *Yearbook of medical informatics* 25.S 01 (2016), S48–S61.

[16] Maged N Kamel Boulos et al. “Mobile medical and health apps: state of the art, concerns, regulatory control and certification”. In: *Online journal of public health informatics* 5.3 (2014), p. 229.

[17] Devin M Mann et al. “COVID-19 transforms health care through telemedicine: evidence from the field”. In: *Journal of the American Medical Informatics Association* 27.7 (2020), pp. 1132–1135.

[18] Roberto Moro Visconti and Donato Morea. “Healthcare digitalization and pay-for-performance incentives in smart hospital project financing”. In: *International journal of environmental research and public health* 17.7 (2020), p. 2318.

[19] Linda Neuhauser and Gary L Kreps. “eHealth communication and behavior change: promise and performance”. In: *Social Semiotics* 20.1 (2010), pp. 9–27.

[20] Sara J Czaja. “Long-term care services and support systems for older adults: The role of technology.” In: *American Psychologist* 71.4 (2016), p. 294.

[21] Christian Matt, Thomas Hess and Alexander Benlian. “Digital transformation strategies”. In: *Business & information systems engineering* 57.5 (2015), pp. 339–343.

[22] Karen Osmundsen, Jon Iden and Bendik Bygstad. “Digital Transformation: Drivers, Success Factors, and Implications.” In: *MCIS*. 2018, p. 37.

[23] World Health Organization et al. “Global strategy on digital health 2020-2025”. In: (2021).

[24] World Health Organization. *The world health report 2000: health systems: improving performance*. World Health Organization, 2000.

[25] World Health Organization et al. *Monitoring the building blocks of health systems: a handbook of indicators and their measurement strategies*. World Health Organization, 2010.

[26] Juan-Luis Londoño and Julio Frenk. “Structured pluralism: towards an innovative model for health system reform in Latin America”. In: *Health Policy* 41.1 (1997), pp. 1–36.

[27] UNDP. *The importance of health information systems*. Accessed: 2022-01-13. URL: `https://www.undp-capacitydevelopment-health.org/en/capacities/focus/health-information-systems/`.

[28] Enrico Coiera. *Guide to health informatics*. CRC press, 2015.

[29] Clemens Scott Kruse et al. “Cybersecurity in healthcare: A systematic review of modern threats and trends”. In: *Technology and Health Care* 25.1 (2017), pp. 1–10.

[30] James G Anderson. “Social, ethical and legal barriers to e-health”. In: *International journal of medical informatics* 76.5-6 (2007), pp. 480–483.

[31] Tony Sahama, Leonie Simpson and Bill Lane. “Security and Privacy in eHealth: Is it possible?” In: *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*. IEEE. 2013, pp. 249–253.

[32] Richard C Alvarez. “The promise of e-Health–a Canadian perspective”. In: *Ehealth international* 1.1 (2002), pp. 1–6.

[33] Gunther Eysenbach. “What is e-health?” In: *Journal of medical Internet research* 3.2 (2001), e20.

[34] Maria Helena da Fonseca et al. “E-health practices and technologies: a systematic review from 2014 to 2019”. In: *Healthcare*. Vol. 9. 9. MDPI. 2021, p. 1192.

[35] Isabella Scandurra et al. “Disturbing or facilitating?–on the Usability of Swedish eHealth Systems 2013”. In: *e-Health–For Continuity of Care*. IOS Press, 2014, pp. 221–225.

[36] Robert L Glueckauf and Mia Liza A Lustria. “E-health self-care interventions for persons with chronic illnesses: Review and future directions.” In: (2009).

[37] Jennifer Rowley. “An analysis of the e-service literature: towards a research agenda”. In: *Internet research* (2006).

[38] Tor Magne Johnsen et al. “Suitability of video consultations during the COVID-19 pandemic lockdown: cross-sectional survey among Norwegian general practitioners”. In: *Journal of Medical Internet Research* 23.2 (2021), e26433.

[39] Charles Friedman et al. “Toward a science of learning systems: a research agenda for the high-functioning Learning Health System”. In: *Journal of the American Medical Informatics Association* 22.1 (2015), pp. 43–50.

[40] Richard J Willke, Laurie B Burke and Pennifer Erickson. “Measuring treatment impact: a review of patient-reported outcomes and other efficacy endpoints in approved product labels”. In: *Controlled clinical trials* 25.6 (2004), pp. 535–552.

[41] Prasanna R Deshpande et al. “Patient-reported outcomes: a new era in clinical research”. In: *Perspectives in clinical research* 2.4 (2011), p. 137.

[42] Food, Drug Administration et al. “Guidance for industry: patient-reported outcome measures: use in medical product development to support labeling claims”. In: *Fed Regist* 74.235 (2009), pp. 65132–65133.

[43] Theresa Weldring and Sheree MS Smith. “Article commentary: patient-reported outcomes (pros) and patient-reported outcome measures (PROMs)”. In: *Health services insights* 6 (2013), HSI–S11093.

[44] Michael Herdman et al. “Development and preliminary testing of the new five-level version of EQ-5D (EQ-5D-5L)”. In: *Quality of life research* 20.10 (2011), pp. 1727–1736.

[45] Ethan Basch et al. “Long-term toxicity monitoring via electronic patient-reported outcomes in patients receiving chemotherapy”. In: *Journal of Clinical Oncology* 25.34 (2007), pp. 5374–5380.

[46] Lena Hohwü et al. “Web-based versus traditional paper questionnaires: a mixed-mode survey with a Nordic perspective”. In: *Journal of medical Internet research* 15.8 (2013), e173.

[47] Sabyasachi Dash et al. “Big data in healthcare: management, analysis and future prospects”. In: *Journal of Big Data* 6.1 (2019), pp. 1–25.

[48] Travis B Murdoch and Allan S Detsky. “The inevitable application of big data to health care”. In: *Jama* 309.13 (2013), pp. 1351–1352.

[49] Bonnie Kaplan. “Seeing through health information technology: the need for transparency in software, algorithms, data privacy, and regulation”. In: *Journal of Law and the Biosciences* 7.1 (2020), lsaa062.

[50] Gary L Kreps and Linda Neuhauser. “New directions in eHealth communication: opportunities and challenges”. In: *Patient education and counseling* 78.3 (2010), pp. 329–336.

[51] D Harrison McKnight and Norman L Chervany. “The meanings of trust”. In: (1996).

[52] Denise M Rousseau et al. “Not so different after all: A cross-discipline view of trust”. In: *Academy of management review* 23.3 (1998), pp. 393–404.

[53] David Mechanic and Mark Schlesinger. “The impact of managed care on patients’ trust in medical care and their physicians”. In: *Jama* 275.21 (1996), pp. 1693–1697.

[54] Angela Coulter. *Patients’ views of the good doctor: doctors have to earn patients’ trust*. 2002.

[55] General Medical Council. *The duties of a doctor registered with the General Medical Council*. General Medical Council, 1998.

[56] Nursing Midwifery Council. *The Code for nurses and midwives*. The Code for nurses and midwives, 2018.

[57] Joanne E Croker et al. “Factors affecting patients’ trust and confidence in GPs: evidence from the English national GP patient survey”. In: *BMJ open* 3.5 (2013).

[58] Bonnie R Sakallaris et al. “Meeting the challenge of a more person-centered future for US healthcare”. In: *Global advances in health and medicine* 5.1 (2016), pp. 51–60.

[59] Mark A Hall et al. “Measuring patients’ trust in their primary care providers”. In: *Medical care research and review* 59.3 (2002), pp. 293–318.

[60] Jan Marco Leimeister, Winfried Ebner and Helmut Krcmar. “Design, implementation, and evaluation of trust-supporting components in virtual communities for patients”. In: *Journal of Management Information Systems* 21.4 (2005), pp. 101–131.

[61] Onora O’Neill. “Intelligent Trust in a Digital World”. In: *New Perspectives Quarterly* 34.4 (2017), pp. 27–31. DOI: `10.1111/npqu.12105`.

[62] Steven D Pearson and Lisa H Raeke. “Patients’ trust in physicians: many theories, few measures, and little data”. In: *Journal of general internal medicine* 15.7 (2000), pp. 509–513.

[63] Pennie Frow, Janet R McColl-Kennedy and Adrian Payne. “Co-creation practices: Their role in shaping a health care ecosystem”. In: *Industrial Marketing Management* 56 (2016), pp. 24–39.

[64] Enid NH Montague, Brian M Kleiner and Woodrow W Winchester III. “Empirically understanding trust in medical technology”. In: *International Journal of Industrial Ergonomics* 39.4 (2009), pp. 628–634.

[65] Dylan Yaga et al. “Blockchain Technology Overview”. In: *National Institute of Standards and Technology, NISTIR 8202, US Department of Commerce, Washington, USA* (2018).

[66] Daniele Rotolo, Diana Hicks and Ben R Martin. “What is an emerging technology?” In: *Research policy* 44.10 (2015), pp. 1827–1843.

[67] Mayank Raikwar, Danilo Gligoroski and Katina Kralevska. “SoK of used cryptography in blockchain”. In: *IEEE Access* 7 (2019), pp. 148550–148575.

[68] Vitalik Buterin et al. “A next-generation smart contract and decentralized application platform”. In: *white paper* 3.37 (2014).

[69] Ivan Bjerre Damgård. “A design principle for hash functions”. In: *Conference on the Theory and Application of Cryptology*. Springer. 1989, pp. 416–427.

[70] Ralph C Merkle. “A certified digital signature”. In: *Conference on the Theory and Application of Cryptology*. Springer. 1989, pp. 218–238.

[71] Ralph C Merkle. *Method of providing digital signatures*. US Patent 4,309,569. Jan. 1982.

[72] Ronald L Rivest, Adi Shamir and Len Adleman. *On Digital Signatures and Public-Key Cryptosystems.* Tech. rep. MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE, 1977.

[73] Don Johnson, Alfred Menezes and Scott Vanstone. “The elliptic curve digital signature algorithm (ECDSA)”. In: *International journal of information security* 1.1 (2001), pp. 36–63.

[74] Mihir Bellare et al. “Relations among notions of security for public-key encryption schemes”. In: *Annual International Cryptology Conference*. Springer. 1998, pp. 26–45.

[75] Nick Szabo. “Formalizing and securing relationships on public networks”. In: *First monday* (1997).

[76] Elli Androulaki et al. “Hyperledger fabric: a distributed operating system for permissioned blockchains”. In: *Proceedings of the thirteenth EuroSys conference*. 2018, pp. 1–15.

[77] Dmitry Tanana. “Avalanche blockchain protocol for distributed computing security”. In: *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE. 2019, pp. 1–3.

[78] Andreas M Antonopoulos and Gavin Wood. *Mastering ethereum: building smart contracts and dapps*. O’reilly Media, 2018.

[79] Chris Dannen. *Introducing Ethereum and solidity*. Vol. 318. Springer, 2017.

[80] E. B. Sasson et al. “Zerocash: Decentralized Anonymous Payments from Bitcoin”. In: *2014 IEEE Symposium on Security and Privacy*. May 2014, pp. 459–474. DOI: `10.1109/SP.2014.36`.

[81] The Monero Project. *Monero*. 2014. URL: `https://web.getmonero.org`.

[82] David Schwartz, Noah Youngs, Arthur Britto et al. “The Ripple protocol consensus algorithm”. In: *Ripple Labs Inc White Paper* 5 (2014).

[83] EOS IO. “EOS. IO technical white paper”. In: *EOS. IO (accessed 18 December 2017) https://github.com/EOSIO/Documentation* (2017).

[84] LTO Network. *Blockchain for Decentralized Workflows*. 2014. URL: `www.lto.network`.

[85] Elli Androulaki et al. “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains”. In: *Proceedings of the Thirteenth EuroSys Conference*. EuroSys ’18. New York, NY, USA: ACM, 2018, 30:1–30:15. ISBN: 978-1-4503-5584-1.

[86] *Monax*. 2014. URL: `https://monax.io/`.

[87] Gideon Greenspan. *MultiChain Private Blockchain*. `https://www.multichain.com/download/MultiChain-White-Paper.pdf`. 2015.

[88] Libra Association. *The Libra Blockchain*. `https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf`. [Online; accessed 24-Jun-2019]. June 2019.

[89] Florian Gräbe et al. “Do not be fooled: Toward a holistic comparison of Distributed Ledger Technology designs”. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*. 2020.

[90] Leo Maxim Bach, Branko Mihaljevic and Mario Zagar. “Comparative analysis of blockchain consensus algorithms”. In: *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE. 2018, pp. 1545–1550.

[91] Cynthia Dwork and Moni Naor. “Pricing via processing or combatting junk mail”. In: *Annual international cryptology conference*. Springer. 1992, pp. 139–147.

[92] Markus Jakobsson and Ari Juels. “Proofs of work and bread pudding protocols”. In: *Secure information networks*. Springer, 1999, pp. 258–272.

[93] Alex de Vries. “Bitcoin boom: What rising prices mean for the network’s energy consumption”. In: *Joule* 5.3 (2021), pp. 509–513.

[94] Vaibhav Sagar and Praveen Kaushik. “Ethereum 2.0 Blockchain in Healthcare and Healthcare Based Internet-of-Things Devices”. In: *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences: PCCDS 2020*. Springer Singapore. 2021, pp. 225–233.

[95] Miguel Castro, Barbara Liskov et al. “Practical byzantine fault tolerance”. In: *OSDI*. Vol. 99. 1999. 1999, pp. 173–186.

[96] Christian Cachin et al. “Architecture of the hyperledger blockchain fabric”. In: *Workshop on distributed cryptocurrencies and consensus ledgers*. Vol. 310. 4. Chicago, IL. 2016.

[97] Zibin Zheng et al. “An overview of blockchain technology: Architecture, consensus, and future trends”. In: *2017 IEEE international congress on big data (BigData congress)*. IEEE. 2017, pp. 557–564.

[98] Sunny King and Scott Nadal. “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake”. In: *self-published paper, August* 19.1 (2012).

[99] Asaph Azaria et al. “Medrec: Using blockchain for medical data access and permission management”. In: *2016 2nd international conference on open and big data (OBD)*. IEEE. 2016, pp. 25–30.

[100] Tim K Mackey et al. “‘Fit-for-purpose?’–challenges and opportunities for applications of blockchain technology in the future of healthcare”. In: *BMC medicine* 17.1 (2019), pp. 1–17.

[101] Marko Hölbl et al. “A systematic review of the use of blockchain in healthcare”. In: *Symmetry* 10.10 (2018), p. 470.

[102] Thomas McGhin et al. “Blockchain in healthcare applications: Research challenges and opportunities”. In: *Journal of Network and Computer Applications* 135 (2019), pp. 62–75.

[103] Ibrar Yaqoob et al. “Blockchain for healthcare data management: opportunities, challenges, and future recommendations”. In: *Neural Computing and Applications* 34.14 (2022), pp. 11475–11490.

[104] Briony J Oates. *Researching information systems and computing*. Sage, 2005.

[105] Paul Johannesson and Erik Perjons. *A design science primer*. CreateSpace, 2012.

[106] Jakob Nielsen. “The usability engineering life cycle”. In: *Computer* 25.3 (1992), pp. 12–22.

[107] U.S Food adn Drug administration. *The Device Development Process*. Accessed: 2021-09-28. URL: `https://www.fda.gov/patients/learn-about-drug-and-device-approvals/device-development-process`.

[108] Daniel Gustafsson et al. “Analysing the Double diamond design process through research & implementation”. In: (2019).

[109] Jan Gulliksen et al. “Key principles for user-centred systems design”. In: *Behaviour and Information Technology* 22.6 (2003), pp. 397–409.

[110] Donald A Norman and Stephen W Draper. “User centered system design: New perspectives on human-computer interaction”. In: (1986).

[111] Chadia Abras, Diane Maloney-Krichmar, Jenny Preece et al. “User-centered design”. In: *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications* 37.4 (2004), pp. 445–456.

[112] Allison Druin. “The role of children in the design of new technology”. In: *Behaviour and information technology* 21.1 (2002), pp. 1–25.

[113] David Moher et al. “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement”. In: *PLoS medicine* 6.7 (2009), e1000097.

[114] Wichor M Bramer, Dean Giustini and Bianca MR Kramer. “Comparing the coverage, recall, and precision of searches for 120 systematic reviews in Embase, MEDLINE, and Google Scholar: a prospective study”. In: *Systematic reviews* 5.1 (2016), pp. 1–7.

[115] Wichor M Bramer et al. “Optimal database combinations for literature searches in systematic reviews: a prospective exploratory study”. In: *Systematic reviews* 6.1 (2017), pp. 1–12.

[116] Antonio Cavacini. “What is the best database for computer science journal articles?” In: *Scientometrics* 102.3 (2015), pp. 2059–2071.

[117] ACM. *ACM about*. Accessed: 2023-01-02. URL: `https://dl.acm.org/about`.

[118] IEEE. *IEEE about*. Accessed: 2023-01-02. URL: `https://guides.library.unlv.edu/engineering/IEEEXplore`.

[119] Yair Levy and Timothy J Ellis. “A systems approach to conduct an effective literature review in support of information systems research.” In: *Informing Science* 9 (2006).

[120] K Prasanna et al. “PoC design: a methodology for proof-of-concept (PoC) development on internet of things connected dynamic environments”. In: *Security and Communication Networks* 2021 (2021).

[121] Michelle Campbell et al. “Framework for design and evaluation of complex interventions to improve health”. In: *Bmj* 321.7262 (2000), pp. 694–696.

[122] Alan R Hevner et al. “Design science in information systems research”. In: *MIS quarterly* (2004), pp. 75–105.

[123] Klaus Pohl. *Requirements engineering: fundamentals, principles, and techniques*. Springer Publishing Company, Incorporated, 2010.

[124] Dhirendra Pandey, U Suman and AK Ramani. “Social-organizational participation difficulties in requirement engineering process: A study”. In: *Software Engineering* 1.1 (2010), p. 1.

[125] Anton Hasselgren. *VerifyMed mock-up*. Online; accessed 28.09.2021. URL: `https://xd.adobe.com/view/0f333da6-62a5-4928-bb32-b919452ff313-5a60/?fullscreen&hints=off`.

[126] Jeffrey Rubin and Dana Chisnell. *Handbook of usability testing: how to plan, design and conduct effective tests*. John Wiley & Sons, 2008.

[127] Martyn Denscombe. *EBOOK: The Good Research Guide: For Small-Scale Social Research Projects*. McGraw-Hill Education (UK), 2017.

[128] Scott W Vanderstoep and Deidre D Johnson. *Research methods for everyday life: Blending qualitative and quantitative approaches*. Vol. 32. John Wiley & Sons, 2008.

[129] JM Christian Bastien. “Usability testing: a review of some methodological and technical aspects of the method”. In: *International journal of medical informatics* 79.4 (2010), e18–e23.

[130] John Brooke et al. “SUS-A quick and dirty usability scale”. In: *Usability evaluation in industry* 189.194 (1996), pp. 4–7.

[131] Patricia I Fusch and Lawrence R Ness. “Are we there yet? Data saturation in qualitative research”. In: *The qualitative report* 20.9 (2015), p. 1408.

[132] Vanessa Azevedo et al. “Interview transcription: conceptual issues, practical guidelines, and challenges”. In: *Revista de Enfermagem Referência* IV Série (Sept. 2017), pp. 159–168. DOI: `10.12707/RIV17018`.

[133] Kirsti Malterud. “Systematic text condensation: a strategy for qualitative analysis”. In: *Scandinavian journal of public health* 40.8 (2012), pp. 795–805.

[134] Hege K Andreassen et al. “Patients who use e-mediated communication with their doctor: new constructions of trust in the patient-doctor relationship”. In: *Qualitative health research* 16.2 (2006), pp. 238–248.

[135] Jens-Andreas Hanssen Rensaa. “VerifyMed-Application of blockchain technology to improve trust in virtualized healthcare services”. Master’s thesis, Norwegian University of Science and Technology (NTNU), 2020.

[136] Aaron Bangor, Philip Kortum and James Miller. “Determining what individual SUS scores mean: Adding an adjective rating scale”. In: *Journal of usability studies* 4.3 (2009), pp. 114–123.

[137] Rong Zhang and Wai Kin Victor Chan. “Evaluation of energy consumption in block-chains with proof of work and proof of stake”. In: *Journal of Physics: Conference Series*. Vol. 1584. 1. IOP Publishing. 2020, p. 012023.

[138] Wei Yan Ng et al. “Blockchain applications in health care for COVID-19 and beyond: a systematic review”. In: *The Lancet Digital Health* 3.12 (2021), e819–e829.

[139] Heather L Colquhoun et al. “Scoping reviews: time for clarity in definition, methods, and reporting”. In: *Journal of clinical epidemiology* 67.12 (2014), pp. 1291–1294.

[140] Gilbert Cockton, Alan Woolrych and Darryn Lavery. “Inspection-based evaluations”. In: *Human-Computer Interaction*. CRC Press, 2009, pp. 289–308.

[141] Cornelius C Agbo, Qusay H Mahmoud and J Mikael Eklund. “Blockchain technology in healthcare: a systematic review”. In: *Healthcare*. Vol. 7. 2. MDPI. 2019, p. 56.

[142] Cardano. *Cardano blockchain*. Online; accessed 02.01.2023. URL: `https://cardano.org`.

[143] Solana. *Solana blockchain*. Online; accessed 02.01.2023. URL: `https://solana.com`.

A

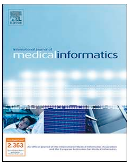
Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S.A. and Faxvaag, A., 2020. Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, p.104040.

International Journal of Medical Informatics 134 (2020) 104040

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.elsevier.com/locate/ijmedinf



Review article

Blockchain in healthcare and health sciences—A scoping review

Anton Hasselgren[a,*], Katina Kralevska[b], Danilo Gligoroski[b], Sindre A. Pedersen[c], Arild Faxvaag[a]

[a] Department of Neuromedicine and Movement Science, Faculty of Medicine and Health Sciences, NTNU-Norwegian University of Science and Technology, Trondheim, Norway
[b] Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU-Norwegian University of Science and Technology, Trondheim, Norway
[c] Library Section for Medicine and Health Sciences, NTNU University Library, NTNU-Norwegian University of Science and Technology, Trondheim, Norway

ARTICLE INFO

Keywords:
Blockchain
Health systems
Scoping review
Distributed ledger

ABSTRACT

Background: Blockchain can be described as an immutable ledger, logging data entries in a decentralized manner. This new technology has been suggested to disrupt a wide range of data-driven domains, including the health domain.

Objective: The purpose of this study was to systematically review, assess and synthesize peer-reviewed publications utilizing/proposing to utilize blockchain to improve processes and services in healthcare, health sciences and health education.

Method: A structured literature search on the topic was conducted in October 2018 relevant bibliographic databases.

Result: 39 publications fulfilled the inclusion criteria. The result indicates that Electronic Health Records and Personal Health Records are the most targeted areas using blockchain technology. Access control, interoperability, provenance and data integrity are all issues that are meant to be improved by blockchain technology in this field. Ethereum and Hyperledger fabric seem to be the most used platforms/frameworks in this domain.

Conclusion: This study shows that the endeavors of using blockchain technology in the health domain are increasing exponentially. There are areas within the health domain that potentially could be highly impacted by blockchain technology.

1. Introduction and rationale

The technology of blockchain, with inherited characteristics such as decentralization, transparency and anonymization, was introduced in the cryptocurrency Bitcoin in 2008 [1]. Bitcoin, with close to 400 million completed transactions (March 19, 2019) [2], represents a solid use-case that blockchain technology works. This has led to discussions and proposals that blockchain technology could be useful in a range of other data-driven domains, including healthcare [3].

According to IBM, 70 % of healthcare leaders predict that the greatest impact of blockchain within the health domain will be improvement of clinical trial management, regulatory compliance and providing a decentralized framework for sharing electronic health records (EHR) [4]. Moreover, the global blockchain technology market in the healthcare industry is expected to cross $500 million by 2022 [61]. Although blockchain technology is considered to have potential for real improvement of health information systems [3], the recent hype surrounding this technology similarly entails unrealistic proposals and ideas and current literature provides little overview of applications that have been developed, tested and/or deployed.

It is valuable to investigate if the current research meets the expectations to blockchain technology within healthcare, health sciences and health education (from hereinafter, referred to as “the health domain”). This study aims to systematically review, assess and synthesize published peer-reviewed studies where blockchain has been utilized (or proposed to be utilized) to improve processes and services within the health domain. In addition to examining the evidence, we also aim to provide an overview of what has been done, what is known, and the potential directions forward on this topic.

The remainder of this paper is organized as follows: Section **two** presents a background of blockchain technology with a description of its key elements and an overview of the problems in the health domain where blockchain potentially could add value. Section **three** outlines the systematic methodology of the study including search strategy, selection process, data extraction, data analysis and quality assessment of the included publications. The results are presented in section **four** with a bibliographic overview and descriptive analysis of the extracted data. Finally, section **five** presents a discussion of the research results in

---

[*] Corresponding author at: Norwegian University of Science and Technology, NTNU, 7491 Trondheim, Norway.
E-mail address: anton.hasselgren@ntnu.no (A. Hasselgren).

https://doi.org/10.1016/j.ijmedinf.2019.104040
Received 13 May 2019; Received in revised form 25 November 2019; Accepted 2 December 2019

the context of the aim and research questions, including strengths and limitations of this study.

2. Background

Blockchain can be described as an immutable ledger that logs data entries in a decentralized manner. It enables entities to interact without the presence of a central trusted third party. The blockchain maintains a continuously growing set of data entries, bundled together into blocks of data. These blocks are, upon acceptance to the blockchain linked to the previous and future blocks with cryptographic protocols [60]. In blockchain's original form, these data records/blocks are; readable by all, writable by all, and tamper-proof by all. This for instance allows decentralized transactions and data management. Due to these properties, blockchain has gained much attention for various applications. Additionally, blockchain allows for smart contracts; self-execution contracts that do not require any central authority. The blockchain Ethereum is at this date the largest facilitator of smart contracts on blockchain [5].

2.1. What is Blockchain

2.1.1. Key characteristics

A key attribute of blockchain is decentralization; no central authority controls the content added to the blockchain. Instead, the entries passed on to the blockchain are agreed upon in a peer-to-peer network using a various consensus protocols (see 2.1.4 Consensus mechanism). Another key characteristic of blockchain is persistency. It is practically impossible to delete entries after being accepted onto the blockchain due to the distributed ledger, stored across multiple nodes [6]. Furthermore, the possibility of anonymity (or pseudonymity) is an appealing characteristic utilized in many blockchains.

Blockchains make audit and traceability possible by linking a new block to the previous by including the hash of the latter, and in this way forming a chain of blocks. The transactions in the blocks are formed in a Merkle tree [7] where each leaf value (transaction) can be verified to the known root. This enables the tree structure to verify the integrity of the data by only storing the root of the tree on the blockchain. Fig. 1 provides a visualization of this basic structure.

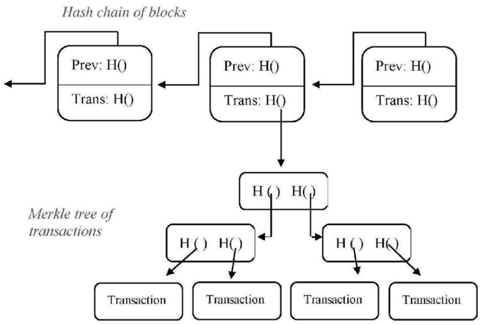


Fig. 1. Blockchain structure.

2.1.2. Type of blockchains

As illustrated in Table 1, there are mainly three types of blockchains: public (permissionless), consortium (public permissioned) and private [6]. They possess different characteristics regarding who can access, write and read the data on the blockchain. The data in a public chain can be viewed by all and anyone can join and contribute to both consensus (in theory) and changes to the core software [6]. The public blockchain is widely used in cryptocurrencies, and the two largest cryptocurrencies: Bitcoin [1] and Ethereum [5] (the main chain), are categorized as public permissionless chains. A consortium blockchain can be considered partially centralized, with only a limited number of selected groups of entities having access to view and participate in the consensus protocol. In a private blockchain, the network is distributed yet often centralized. Only selected nodes can participate in the network and they are often managed by one central authority [6]. The debate around the definition and the categorization of different types of blockchains presented here is ongoing. Currently, there is no broad consensus of which distributing qualities and consensus mechanisms are required to label a technology as "blockchain" [8].

2.1.3. Existing or new blockchains

There are currently existing blockchain frameworks and platforms that can be utilized for development of decentralized applications (dapps). Ethereum (decentralized platform) (5) and Hyperledger (framework) [9] are so far the most popular, and both allow developers to build new blockchain applications onto existing blockchains and to create new test-nets using their protocols.

2.1.4. Consensus mechanisms

A key component of blockchains is the way data entries are accepted onto the distributed ledger by a distributed consensus protocol validating the data entries. Several proposed and used consensus protocols exist, of which the three most commonly used are illustrated in Table 2 and presented in the following:

Table 2
Consensus mechanisms comparison [6].

Property	PoW	PoS	PBFT
Node management	Open	Open	Permissioned
Energy consumption	High	Medium	Low
Tolerated power of adversary	$< 25\%$ computing power	$< 51\%$ stake	$< 33.3\%$ faulty replicas
Example	Bitcoin [1]	Peercoin [13]	Hyperledger Fabric [12]

Proof-of-Work (PoW) is the consensus protocol most strongly associated with blockchain due to its integration in Bitcoin. When PoW protocol applies, so-called miners are competing in solving a computational hard puzzle. Using brute force, the miners try to find a hash of the proposed block with a value lower than a predetermined one. The miner who first computes this hash value validates the transactions (or other entries) within the block and gets an award (1). A major drawback of the PoW protocol is its energy demanding nature when applied

Table 1
Type of blockchains overview [6].

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

on a large blockchain. This is illustrated by the fact that the current electricity consumed for Bitcoin mining is comparable to the electricity requirements of a smaller country [10].

With **Proof of Stake** (PoS), the selection of an approving node is determined by the stake each node has in the blockchain. For cryptocurrencies, the stake is represented by the balance one possesses of a given currency. This, however, might give an unfair advantage to the "richest" node. To account for this, several hybrid versions of PoS have been suggested where the stake is combined with some randomization to select the approving node. The second largest cryptocurrency Ethereum is planning to move from PoW to PoS [6].

Practical Byzantine Fault Tolerance (PBFT) is based on a Byzantine agreement protocol [11]. In PBFT, all nodes need to be known to the network, which limits the usage of this consensus protocol in a public blockchain. Three phases can be defined in the PBFT consensus process: pre-prepared, prepared and commit. Each node needs two thirds of the votes from all nodes to move through the three phases. PBFT is currently used in Hyperledger Fabric [12].

2.1.5. Smart contracts

Some blockchain infrastructures like Ethereum support smart contracts [5]. These are self-executing contractual agreements where pre-agreed upon provisions are formalized in source code. Since smart contracts are automatically enforced based on these pre-agreed provisions they work without any third party or intermediate. This function within a smart contract can be awoken in a blockchain transaction and the use of this functionality seems to be appealing to the health domain [5].

2.2. The potential of blockchain in the health domain

The healthcare sector is a problem-driven, data- and personnel-intensive domain where the ability to access, edit and trust the data emerging from its activities are critical for the operations of the sector as a whole. If we divide the operations within the healthcare sector into triage, health problem-solving, clinical decision-making, realization and assessment of knowledge-based care (Fig. 2), achieving the desired health outcomes hinges on engaging a multidisciplinary team of health personnel that apply the most appropriate knowledge, technologies and skills when dealing with the patient. When collaborating with educational institutions, the healthcare sector must provide access to patients and provide an arena for training so that students can develop and refine the necessary skills. In return, the educational institutions provide the sector with qualified personnel. When collaborating with institutions and companies with a research and engineering agenda, health institutions must assist in providing access to professionals, informants, test persons and samples. When participating in prospective clinical trials, health institutions must assist in developing, planning, conducting and reporting the experiments. In return, the research and engineering institutions provide the healthcare sector with updated knowledge, methods and tools. Hence, the activities of health institutions are tightly interwoven with institutions engaged in educating health personnel and in biomedical research and engineering (Fig. 2). The activities require effective interchange of consents, patient-related data and proofs, and reimbursements processes, which effectively means exchanging data across institutional borders. At the same time, health institutions are mandated to protect the highly sensitive data that patients choose to share with them.

To both maintain the patient's privacy and exchange data with other institutions in the healthcare ecosystem, access control, provenance, data integrity and interoperability are crucial. The traditional way of achieving **access control** commonly assumes trust between the owner of the data and the entities storing them. These entities are often servers fully entrusted for defining and enforcing access control policies [14]. **Interoperability** is the ability of different information systems, devices or applications to connect, in a coordinated manner, within and across organizational boundaries to access, exchange and cooperatively use

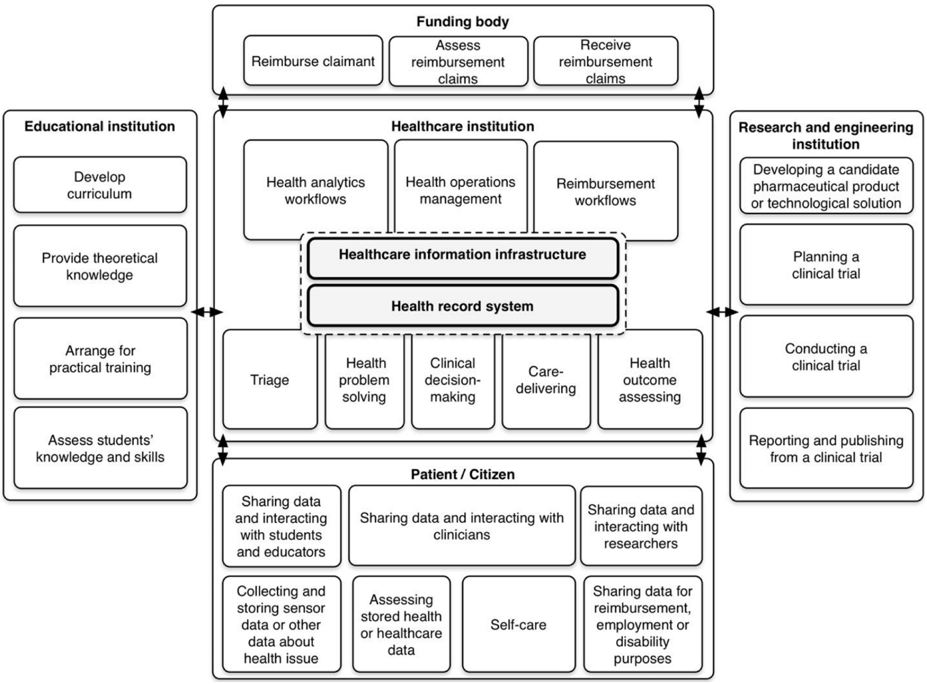


Fig. 2. Map of the health sector.

data amongst stakeholders, with the goal of optimizing the health of individuals and populations. **Data provenance** refers to the historical record of data and their origins. In the health domain data, provenance can, for example, be to deliver auditability and transparency in EHR, and to achieve trust in EHR software system. **Data integrity** as a general definition given by Courtney and Ware is the data quality definition which deals with the expected quality of the data [15]. This means that the degree to which the expected quality of the data is meet or exceeded determines the data integrity.

Healthcare institutions currently experience an increased demand of real-world data from industry and research organizations [16]. At the same time, unauthorized sharing, and highly publicized break-ins and robbery of sensitive data constantly erode the public trust in healthcare institutions. A third problem is malpractices within the healthcare ecosystem that exploits the very same trust (e.g. the problems with counterfeit drugs, procedures, skills and patients). Taken together, this is a situation that commands rethinking and consideration of alternative approaches. With some of its key attributes such as decentralization, distribution and data integrity, and without any necessary third party, blockchain technology has many appealing properties that could be utilized to improve and obtain a higher level of interoperability, information sharing, access control, provenance and data integrity among the mentioned stakeholders, thereby moving towards a new infrastructure for building and maintaining trust.

3. Method

3.1. Search strategy

A structured literature search on the topic was conducted in the following bibliographic databases with the aid of a medical research librarian [SAP]: MEDLINE, Embase, Cochrane Library, Scopus, Google Scholar, Compendex, Inspec, ACM and IEEE. The search strategy compromised searching for free-text terms for the concept "blockchain" within health topic databases. In the other databases, the concept "blockchain" was combined with the concept "health" using the Boolean operator AND. Within the concepts, word variants and related terms were covered and combined using the Boolean operator OR. Backward and forward search (snowballing method) [17] was applied for the included papers to further assure that all relevant sources were exhausted. This process applied on all included papers and considered complete when no new additional, relevant papers were found. The literature search was last updated 10th October 2018. All references from the databases were exported to EndNote (version x9.1) for duplicate removal and final screening. The search targeted published research in scholarly journals, conference proceedings and workshop reports that asses blockchain concepts within the health domain. For a complete overview over the applied search see Appendix A – Search strategy.

3.2. Selection process

Titles, abstracts and full articles were subsequently screened by reviewer 1 [AH] applying the inclusion and exclusion criteria (Appendix B – Protocol). Publications meeting the inclusive criteria, and those for which the first reviewer was in doubt, were reviewed a second time by three additional reviewers [AF, KK and DG]. In cases of disagreement, a discussion between all four reviewers determined inclusion or exclusion. Fig. 3 illustrates the process.

3.3. Data extraction

Data was extracted from the included papers in a pre-development matrix. The data extraction was mainly done by reviewer 1 [AH] and later re-examined by reviewers 2–4 [AF, KK and DG]. The extracted data was categorized and summarized in the matrix and later exported into tables and graphs. The data matrix was developed in Google Sheet for a convenient workflow within the research group and later exported to Microsoft Excel (version 16.16.5).

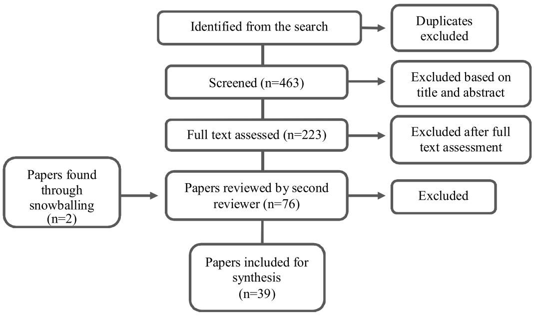


Fig. 3. Inclusion flowchart.

3.4. Data analysis

Relevant extracted quantified data was summarized. The data analysis was completed in Microsoft Excel (version 16.16.5). Where applicable, mean with standard deviation (SD) was calculated (expressed as ±). All numbers were rounded off to the closest integer. All categorical data are expressed as percentage if not stated otherwise.

3.5. Quality assessment

As an important part of the review process a meticulous quality assessment of included publications was conducted [17]. Since developed and validated tools for assessing the different methodologies of the included publications are lacking, development of a specific tool to serve the purpose was necessary. To this end, parts of the method presented by Hölbl et al. were used and modified as appropriate [18]. No papers were excluded in the quality assessment process. The papers received a score based on the criteria (Table 3). The score was given as follows: (NO or SCARCELY) = 0, (MODERATELY) = 1, (YES or ADEQUATELY) = 2. The process of quality assessment was done by reviewer 1 [AH] and later independently pre-reviewed by reviewers 2–4 [AF, KK and DG].

Table 3
Quality assessment tool adapted from Hölbl et al. [18].

Quality Assessment Query	Indicator (0–2)
Q2 Is the health domain problem described?	No-Moderately-YES
Q2 Are the research objectives clearly outlined?	No-Moderately-YES
Q3 Are the main contributions well described?	No-Moderately-YES
Q4 How appropriate is the problem-solution fit?	Scarcely-Moderately-Adequately
Q5 Are the proposed solutions feasible (scalable, economical, implementable)?	No-Moderately-YES

4. Results

The following section presents a summary of the extracted data from the included papers (n = 39).

4.1. Bibliographic overview

As shown in Table 4, the included publications seem to be evenly distributed between journal publications and conference proceedings. IEEE Access with five papers and The Journal of Medical Systems with six papers represented the journals with most included publications. All included papers presented a study design that could be categorized as a

Table 4
Bibliographic overview of the included studies.

Id, reference	Name of first author	Year of publication	Publication type	Publisher	Main contribution	Study design
1 [19]	Zhang, Peng	2018	Journal	Computational and Structural Biotechnology Journal	Structural design	Proof-of-Concept/Case-study
2 [20]	Shan, Jiang	2018	Conference proceeding	IEEE International conference on smart computing	Algorithm/Protocol	Proof-of-Concept
3 [21]	Kleinaki, Athina-Styliani	2018	Journal	Computational and Structural Biotechnology Journal	Structural design	Proof-of-Concept/Case-study
4 [22]	Peterson, Kevin	2016	Conference proceeding	Proc. NIST Workshop Blockchain Healthcare	Algorithm/Protocol	Proof-of-Concept
5 [23]	Ichikawa, Daisuke	2017	Journal	JMIR Mhealth and Uhealth	Structural design	Proof-of-Concept/Case-study
6 [24]	Patel, Vishal	2018	Journal	Health informatics journal	Structural design	Proof-of-Concept
7 [25]	Zhang, Jie	2016	Journal	IEEE Access	Security protocols	Proof-of-Concept
8 [26]	Roehrs, Alex	2017	Journal	Journal of biomedical informatics	Structural design	Proof-of-Concept
9 [27]	Liang, Xueping	2017	Conference proceeding	2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications	Structural design	Proof-of-Concept
10 [28]	Zhang, Aiqing	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept
11 [29]	Rahman, Abdur	2018	Journal	IEEE Access	Structural design	Proof-of-Concept
12 [30]	Gue, Rui	2017	Journal	IEEE Access	Algorithm/Protocol	Proof-of-Concept
13 [31]	Xia, Qi	2017	Journal	IEEE Access	Structural design	Proof-of-Concept
14 [32]	Zhou, Lijing	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept/Case-study
15 [33]	Azaria, Asaph	2016	Conference proceeding	International conference on open and big data	Structural design	Proof-of-Concept
16 [34]	Hussein, Ahmed,	2018	Journal	Cognitive Systems Research	Algorithm/Protocol	Proof-of-Concept
17 [35]	Zhao, Huawei	2017	Conference proceeding	2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)	Algorithm/Protocol	Proof-of-Concept/Case-study
18 [36]	Fan, Kai	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept
19 [37]	Mikula, Tomas	2018	Conference proceeding	2018 21 st Euromicro Conference on Digital System Design	Algorithm/Protocol	Proof-of-Concept/Case-study
20 [38]	Wang, Hao	2018	Journal	Journal of medical systems	Structural design/cryptographic primitive	Proof-of-Concept
21 [39]	Griggs, Kristen	2018	Journal	Journal of medical systems	Structural design	Proof-of-Concept
22 [40]	Dias, Joao Pedro	2018	Journal	arXiv	Structural design	Proof-of-Concept
23 [41]	Dagher, Gaby G	2018	Journal	Sustainable cities and society	Structural design/framework	Proof-of-Concept/Case-study
24 [42]	Chen, Jieying	2018	Conference proceeding	IEEE International Symposium on Innovation and Entrepreneurship	Structural design	Proof-of-Concept
25 [43]	Bocek, Thomas	2017	Conference proceeding	IFIP/IEEE Symposium on Integrated Network and Service Management	Structural design/framework	Proof-of-Concept/Case-study
26 [44]	Angeletti, Fabio	2017	Conference proceeding	25th International Conference on Software, Telecommunications and Computer Networks	Structural design	Proof-of-Concept
27 [45]	Theodouli, Anastasia	2018	Conference proceeding	17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications	Structural design	Proof-of-Concept
28 [46]	Nugent, Timothy	2016	Journal	F1000Research	Structural design	Proof-of-Concept
29 [47]	Momoshina, Polina	2018	Journal	Oncotarget	Structural design/framework	Proof-of-Concept
30 [48]	Liang, Xueping	2018	Conference proceeding	International Conference on Information and Communications Security	Algorithm/Protocol	Proof-of-Concept
31 [49]	Li, Hongyu	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept
32 [50]	Laskowski, Marek	2017	Conference proceeding	International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior	Structural design	Proof-of-Concept
33 [51]	Ji, Yaxian	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept/Case-study
34 (52)	Zhang, Xiaoshuai	2018	Conference proceeding	IEEE International Conference on Communications	Algorithm/cryptographic primitive	Proof-of-Concept
35 [53]	Xia, Qi	2017	Journal	Information	Structural design/framework	Proof-of-Concept
36 [54]	Uddin, Ashraf	2018	Journal	IEEE Access	Algorithm/Protocol	Proof-of-Concept/Case-study
37 [55]	Sun, You	2018	Conference proceeding	27th International Conference on Computer Communication and Networks	Algorithm/Protocol	Proof-of-Concept
38 [56]	Rahmadika, Sandi	2018	Journal	International Journal of Engineering Business Management	Algorithm/Protocol	Proof-of-Concept
39 [57]	Zhang, Peng	2017	Journal	arXiv	Structural design/framework	Proof-of-Concept/Case-study

Proof-of-Concept design. In addition, eleven of the included papers could be considered as a hybrid between a Proof-of-Concept and a Case-study design. The included papers were published during the following years; 2016 (n = 4), 2017 (n = 11) and 2018 (n = 23). Most studies were associated with Chinese research institutes or research groups (42 %) followed by institutes and groups in the USA (20 %). The papers had an average citation count of 21 ± 40 (up to March 2019).

The main contributions of the included publications were categorized as illustrated in Table 4. A large proportion proposed a structural design (54 %) as main contribution, followed by proposals including new algorithms or protocols (38 %) (Table 4).

4.1.1. Summary of proposed solutions

The included publications described several systems, processes and challenges in the health domain in which blockchain enhanced concepts were suggested as part of the solution. The most frequently targeted system was EHR, with 43 % of the publications addressing this topic. Other systems of focus were PHR (15 %) and clinical trial support systems (5 %). The processes within the target systems were mostly focused on sharing, storage, exchange and access of medical data. More than half of the publications (62 %) addressed some processes of sharing health data. Many of the PHRs were proposed as patient-controlled and not tethered to a particular health institution or system (Table 6).

4.1.2. Challenges which blockchain aims to improve

As illustrated in Table 5, blockchain was suggested as an improvement to **access control** in 35 % of the included publications. For

Table 5
Summary of proposed solutions impacted by blockchain technology.

Id, ref.	Health Information system	Process that is to be improved	Main challenge that is addressed
1 [19]	Electronic health records	Shared decision making	Interoperability, access control, data integrity
2 [20]	Electronic health records	Health data recording, storing and sharing	Access control, interoperability
3 [21]	Knowledge infrastructures	Aid decision-making by presenting knowledge	Data integrity, repudiation
4 [22]	Electronic health records	Sharing of healthcare information for clinical and research purposes	Access control, interoperability
5 [23]	Personal health records	M-health data recording, storing and sharing	Data integrity, data provenance
6 [24]	Picture archiving and communications systems	Exchange of medical images	Access control
7 [25]	IoT data management/Personal health data	Remote collection and storage of health data	Data integrity, access control
8 [26]	Personal health records	Sharing healthcare data between health institutions	Interoperability, data provenance
9 [27]	Personal health records	Automatic collection, storage and patient-controlled sharing of personal health data	Access control, interoperability
10 [28]	Personal health records	Sharing of health data for use by more than one healthcare institution	Access control, interoperability
11 [29]	Automated diagnostic service for patients	Collection and storage of data about symptoms of dyslexia for the purpose of automated diagnostics, decision-support and research.	Access control, data integrity, interoperability
12 [30]	Electronic health records	Sharing healthcare data between health institutions	Data integrity
13 [31]	Electronic health records	Sharing healthcare data between health institutions	Data integrity, access control
14 [32]	Administrative systems	Sharing healthcare information for administrative or economic purposes	Data integrity, data provenance
15 [33]	Electronic health records	Sharing healthcare data for clinical and research purposes. Recording and sharing of contracts/agreements.	Access control, interoperability, data integrity
16 [34]	Electronic health records	Sharing healthcare (health record) information for clinical, research and administrative [economic] purposes.	Access control, interoperability
17 [35]	Personal health records	Collecting and sharing [health-related] sensor data for clinical purposes.	Interoperability
18 [36]	Electronic health records	Sharing healthcare data for clinical and research purposes.	Access control, interoperability
19 [37]	Electronic health records/ Administrative system	Sharing healthcare data for administrative or economic purposes	Identity management, access control
20 [38]	Electronic health records	Patient data management and storage in a cloud environment	Access control, data integrity, data provenance
21 [39]	Population health management system	Collection and storage of sensor data for remote patient monitoring purposes	Data integrity, data provenance
22 [40]	Personal health data/Electronic health records	Managing access to personal health data and electronic health records	Access control, data integrity
23 [41]	Electronic health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Access control, data integrity, interoperability
24 [42]	Electronic health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Interoperability, access control
25 [43]	Pharma supply-chain	Monitoring the distribution of drugs in a pharmaceutical supply chain.	Data integrity, data provenance
26 [44]	Clinical Trial Support Systems	Recruitment of patients to clinical trials	Data integrity, data provenance
27 [45]	Electronic health records	Sharing healthcare data for clinical and research purposes	Interoperability, data provenance
28 [46]	Clinical Trial Support Systems	Sharing healthcare information for research purposes	Data integrity, data provenance
29 [47]	Research support systems	Establishing a patient-controlled marketplace for selling and buying of healthcare information for research purposes	Access control, interoperability
30 [48]	Personal health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Access control, privacy, data integrity
31 [49]	Electronic health records	Health record storing	Data integrity, privacy
32 [50]	Infectious disease surveillance system	Public health management (monitoring the outbreak of infectious diseases)	Data integrity, data provenance
33 [51]	Telemedicine system	Finding the patient in the context of telemedicine services	Data integrity
34 [52]	Electronic health records	Retrieving information in the EHR	Access control, data integrity
35 [53]	Electronic health records	Sharing healthcare data for clinical and research purposes	Access control, security, interoperability
36 [54]	Personal health records	Patient-controlled collection and sharing of sensor data	Access control, data integrity
37 [55]	Electronic health records	Sharing healthcare data between health institutions	Data provenance
38 [56]	Electronic health records	Patient-controlled sharing of health data between healthcare providers	Access control, interoperability
39 [57]	Electronic health records	Exchange of healthcare data for clinical and research purposes	Access control, interoperability

Table 6
Healthcare information systems that are impacted by blockchain technology.

Information system category	Count	Proportion
Electronic health records	17	43 %
Personal health records	6	15 %
Clinical Trial Support Systems	2	5 %
Knowledge infrastructures	1	3 %
Picture archiving and communications systems	1	3 %
IoT data management/Personal health data	1	3 %
Automated diagnostic service for patients	1	3 %
Administrative systems	1	3 %
Electronic health records/Administrative system	1	3 %
Population health management system	1	3 %
Pharma supply-chain	1	3 %
Grand Total	**39**	

example, in the paper by Patel [24], access to the data (medical images) were provided by requesting and approving transactions of the data (stored off-chain) with private and public keys. Another approach was suggested by Peterson et al. [22], where access is granted by querying data on the blockchain and retrieving it with FHIR URLs once located. Hyperledger Fabric membership service was used by Liang et al. [27] for issuing enrollment certificate and transaction certificate for access control.

Blockchain solutions for the **interoperability** challenges were discussed in several papers (27 %) (Table 5). For example, interoperability was achieved by referencing FHIR resources (URLs) in some solutions [22,19]. Another approach was to provide a translator component as a gateway of the data blocks, translating formats using a different standard [26].

The ability to improve **provenance** was targeted in 12 % of the included publications (Table 5). In a blockchain concept for medical supply chains, data provenance was enhanced by the use of trusted IoT devices that execute smart contracts on the blockchain [43]. Other examples were found in the concepts addressing clinical trials, where data provenance issues are targeted by providing a tracking system of data used in the trials [44,46].

To increase **data integrity** a blockchain solution was proposed in 28 % of the included publications in this review (Table 5). Generally, the data integrity was maintained by the immutability property of the blockchain (2.1.1 – Key characteristics). Data integrity was enhanced by storing hashed medical data or hash pointer on chain [49,41,38]. Another approach for using blockchain to maintain data integrity was found within clinical trials where smart contracts and integration with trusted IoT devices are used [44,46].

4.2. *Technical details of the proposed blockchain concepts*

4.2.1. *Type of blockchain*

A consortium blockchain (38 %) was the preferred type among the included publications. Although several of the papers failed to define their approach (26 %), private- (10 %) and public blockchains (15 %) appears to be less used in the health domain (Fig. 4).

4.2.2. *Blockchain platform/framework*

Ethereum was utilized in eleven (28 %) of the 39 included publications, Hyperledger Fabric four times (10 %) and Exonum once (4 %) (Fig. 4). 14 studies (36 %) developed a new blockchain for their respective concepts. Eight (21 %) of the included studies failed to specify a platform or framework for their concept (Fig. 4).

4.2.3. *Consensus algorithm*

The summarized results indicate that a variety of consensus algorithms are used for blockchain concepts in the health domain (Table 7). The most frequent used consensus algorithm in the included publications were PoW, accounting for 21 % of the cases. In addition, it is also noteworthy that not all concepts that are built using the Ethereum platform or Ethereum protocols used PoW. The second most frequent used consensus algorithm was PBTF (15 %). Several (41 %) of the publications failed to state which consensus protocol their concept intended to apply.

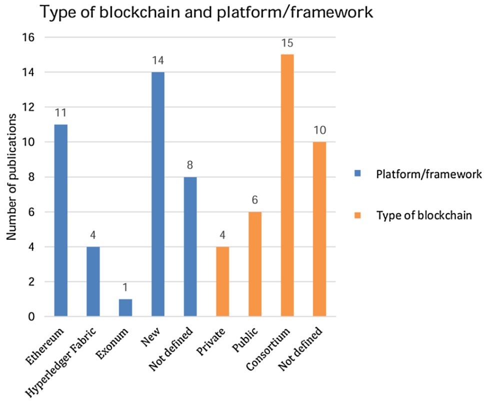


Fig. 4. Type of blockchain and platform/framework.

4.2.4. *Smart contracts*

In several of the proposed concepts, smart contracts were a feature: 38 % of the included studies used smart contracts for some functionality; the remaining studies did not define if smart contracts were a feature or not (Table 7).

Table 7
Usage of consensus algorithm and smart contracts.

Consensus algorithm	Count	Id
Proof of Work (PoW)	8	2, 3, 15, 22, 31–33, 38
Proof of Work (by pre-selected miner)	1	36
Practical Byzantine Fault Tolerance (PBFT)	6	5, 8, 14, 21, 24, 37
Proof of Stake (PoS)	1	6
Proof of Interoperability	1	4
Proof of Conformance	1	10
Permissioned Voting-based	2	19, 20
Ledger-based Byzantine Fault Tolerance	1	29
Hybrid (Delegated PoS + PBFT)	1	18
QuorumChain consensus	1	23
Not defined	16	1, 7, 8, 11–13, 16, 17, 25–28, 30, 34, 35, 39
Use of smart contracts		
Yes	15	1, 3, 4, 13, 15, 19, 21, 23, 25, 27, 28, 29, 31, 32, 39
Not defined	24	2, 5, 6–12, 14, 16–18, 20, 22, 24, 26, 30, 33-38

4.3. *Quality assessment*

Table 8 presents the results of the quality assessment. The maximum number of total points is ten and the minimum is zero. The average score for Q1 (1.0 ± 0.7), Q2 (0.9 ± 0.7) and Q3 (1.0 ± 0.5) appears to be lower than Q4 (1.6 ± 0.6) and Q5 (1.2 ± 0.6). The quality of the included publications varies with a standard deviation of 1.8 for the total mean score and a range of 1–9.

As shown in Fig. 5, the average quality increased in papers

Table 8
Quality assessment.

Id (ref)	Year	Q1 Feasibility	Q2 Problem description	Q3 Research objectives	Q4 Contribution description	Q5 Problem solution fit	Total score
4 [22]	2016	1	1	2	2	1	7
7 [25]	2016	2	1	0	2	0	5
15 [33]	2016	1	1	1	0	2	5
28 [46]	2016	0	0	1	0	0	1
5 [23]	2017	1	0	1	2	1	5
8 [26]	2017	1	2	0	2	1	6
9 [27]	2017	0	1	0	1	2	4
12 [30]	2017	2	0	1	2	1	6
13 [31]	2017	1	2	1	1	2	7
17 [35]	2017	0	0	1	2	1	4
25 [43]	2017	0	0	1	1	1	3
26 [44]	2017	1	0	1	1	1	4
32 [50]	2017	0	0	0	1	0	1
35 [53]	2017	1	1	1	1	2	6
39 [57]	2017	1	0	1	1	1	4
1 [19]	2018	1	2	1	2	2	8
2 [20]	2018	1	1	1	2	1	6
3 [21]	2018	2	1	1	2	2	8
6 [24]	2018	2	1	1	1	1	6
10 [28]	2018	1	2	1	2	1	7
11 [29]	2018	2	2	1	1	1	7
14 [32]	2018	2	2	1	2	1	8
16 [34]	2018	1	0	1	2	1	5
18 [36]	2018	1	1	1	2	2	7
19 [37]	2018	1	2	1	2	1	7
20 [38]	2018	1	0	1	2	1	5
21 [39]	2018	1	1	1	1	1	5
22 [40]	2018	1	0	1	2	1	5
23 [41]	2018	1	2	2	2	2	9
24 [42]	2018	2	1	1	0	1	5
27 [45]	2018	0	0	1	2	1	4
29 [47]	2018	2	1	2	2	2	9
30 [48]	2018	0	1	2	2	1	6
31 [49]	2018	1	0	1	2	1	5
33 [51]	2018	1	1	1	2	2	7
34 [52]	2018	0	1	1	2	1	5
36 [54]	2018	2	1	2	2	2	9
37 [55]	2018	0	1	1	2	2	6
38 [56]	2018	1	1	1	2	1	6
Mean (SD)		1.0 ± 0.7	0.9 ± 0.7	1.0 ± 0.5	1.6 ± 0.6	1.2 ± 0.6	5.7 ± 1.8

published in 2018 compared to 2016 and 2017. Fig. 5 indicates the quality trend of the included publications.

5. Discussion

In this scoping literature review, we have found that the research on the explorative use of blockchain in healthcare is an academic research topic in its infancy but that the number of research groups approaches and proposed solutions currently is growing exponentially. The quality of the papers is also on the rise (Fig. 5). Many researchers explore the use of Smart-contracts on the Ethereum platform, organized as a consortium blockchain. Most of the proposed solutions are implemented in Institution-controlled EHRs, in Personal health record systems (PHRs) or in the mHealth domain. Judged from the number of blockchain-related publications on Google Scholar, the inauguration and growth of blockchain in healthcare as an academic field is in line with those in other academic sectors.

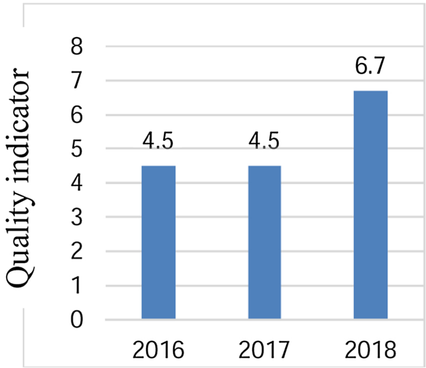


Fig. 5. Average quality score per year.

The utilization of smart-contracts partly explains why Ethereum is the mostly used platform for the proposed concepts (Fig. 4). A smart-contract function, which often has the purpose of reducing third party interaction, has the potential of making health informatic processes more efficient. However, none of the included papers contained evidence of such effect (More research and further exploration of the efficiencies of smart contracts compared to current solutions should be undertaken). In addition to Ethereum, Hyperledger was a popular platform/framework used in the included publications. This correlates well with the overall popularity of blockchain platforms. The reasons for this can be both the attributes that are offered by the respective platform, but also the number of developers available with knowledge on each platform as well as the strong overall market position of Ethereum and Hyperledger. Furthermore, a consortium blockchain appears to be the preferred design choice when it comes to type of blockchain. Since HIS deals with highly sensitive data [18], which usually entails that a limited number of entities should have access, a consortium blockchain may be more appropriate than a public permissionless and private to ensure that data are not accessible by those who have no view rights and also to comply with current health data regulations.

Most papers envisioned the use of blockchain in health record systems (EHRs and PHRs) (Table 6). Within these, the use of blockchain to build functionality for sharing of data within clinical teams and between clinicians and researchers were the most targeted use cases. With stronger emphasis on team-based care and continuity of care across institutional borders, and identity management and access control across different health systems, the processes of sharing becomes important [58]. Four publications [25,27,28,48] proposed to use blockchain for building a personal health record system that could bridge the gap between the patient and institution-specific EHRs. This is an alternative take on the use of health information to fix a broken healthcare system and improve the continuity of care [59] which builds on the patient in a more empowered and controlling role.

Five of the publications addressed the m-health domain and patient-controlled collection, storage and sharing of sensor data [23,27,35,39,32]. The collection and sharing of sensor data is relevant to all virtualized care scenarios (e.g. telecare, remote patient monitoring and population health), and technologies that can make sensor data more to be trusted upon are worthy of exploration. Although these five included publications do not provide enough collective evidence that blockchain may be superior to existing solutions, they provide an insight into an interesting use-case for several reasons; M-health is a rather new field and lacks a common data infrastructure and, to some degree, lacks common regulation around dealing with health data and getting the data accepted by the established health system. There is a reasonable assumption that m-health will increase at a rapid pace in the coming years and the need to verify and access m-health generated data by the health systems becomes crucial for the continued development of HIS and to insure that these data-driven systems stay up to date. The evidence collected in this review gives a clear indication that blockchain enhanced solutions for this area of the health system have a promising potential and needs to be explored further.

Three papers addressed the sharing of clinical data for use in non-clinical contexts [29,32,47]. Most of the use cases were related to biomedical research. Also, two publications explored the use of blockchain in clinical trial systems [44,46]. Hence, the use of blockchain to build better support for basic and translational biomedical research appear to be a well-recognized problem. As illustrated in Fig. 3, institutions that conduct biomedical research are an example of an institution that support and supply healthcare. Taken together, these constitute an ecosystem whose operations are tightly interwoven with those within the healthcare institutions proper. Most interactions involve the use of data that the patient has shared for purposes other than providing or assessing care. We found no publications on the use of blockchain in the context of interaction between patients and healthcare students in the context of healthcare education and training. Also, we found no publications on the use of blockchain for reimbursement purposes. We believe that the use of blockchain-based solutions also should be explored in these application areas. Furthermore, neither of the included publications described how their blockchain-based solution was compliant with GDPR, HIPAA or other national health data laws and regulations. This needs to be explored further to assess the implementation possibilities of blockchain technology within the health domain.

The strength of this publication is its stringent inclusion criteria and the quality assessment approach. This has enabled us to look beyond the mere publishing of thoughts and ideas and instead highlight what has actually been developed, tested and published in a peer-review setting.

The aim of this review was to summarize the peer-reviewed literature under the topic of blockchain in the health domain. Although this study provides a good overview of what has recently been investigated in an academic (peer-reviewed) setting, the review does not capture the whole picture of the development in the area. There are promising developments in the private sector in other areas of the health sector that are not covered in the included publications for this review; for example, genome management and medical credential systems.

Future research on the topic should consider adding more technical details to further enable feasibility assessment and decrease the gap between concepts and implementations, thus moving the technology forward in this area. In addition, further research should also address how blockchain-based solutions can be made to comply with current health data laws and standards. There is a need to explore which blockchain features and designs are suitable under these laws and standards, and which are not to further increase real-world implementation feasibility.

6. Conclusion

Research on the use of blockchain in healthcare is now established as an academic field, and the number and quality of publications are increasing rapidly. This trend is also noticeable in the global healthcare industrial sector, where the blockchain technology market is expected to cross $500 million by 2022. Due to the over-arching importance of maintaining trust while satisfying an ever-increasing demand for exchange of data within the healthcare ecosystem, healthcare institutions are in critical demand for new and improved trust-preserving solutions. The frontier of research, as portrayed in this review, show that blockchain-based solutions currently are being explored in a few EHR, PHR and Clinical trial system use cases. Several other health information system domains are under-explored as we found few if any publications on Knowledge infrastructures, Picture archiving and communications systems, Automated diagnostic service for patients, Administrative systems, Population health management system and Pharma supply-chains. The research agenda needs to be broadened to address these concrete areas, as well as to address the quest for blockchain-based solutions that preserve trust by mitigating threats from within as well from outside the healthcare sector.

Author contributions

All authors have made a substantial, direct, intellectual contribution to this study.

Summary points

What was already known on the topic?

- Blockchain technology has proven to work in cryptocurrencies like Bitcoin.
- The health sector has been one area outside of cryptocurrencies were blockchain technology have been proposed to add value.

What this study added to our knowledge?

- Blockchain-based solutions can improve and simplify the sharing of health record information from Electronic Health Record and Personal Health Record systems.
- Research on Blockchain-based solutions in healthcare is taking pace but it is still in its infancy, as many potential and promising areas remain under-researched and unexploited.

;1;

Declaration of Competing Interest

None.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sector.

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.ijmedinf.2019.104040.

References

[1] S. Nakamoto, Bitcoin: a Peer-to-Peer Electronic Cash System, (2008).

[2] blockchain.com [cited 2019 09.03]. Available from: https://www.blockchain.com/charts/n-transactions-total.

[3] Blockchain technology in healthcare: the revolution starts here. e-health networking, applications and services (Healthcom), in: M. Mettler (Ed.), 2016 IEEE 18th International Conference on, IEEE, 2016.

[4] Health rallies for blockchains: Keeping patients at the center: IBM; 2016 [cited 19.03 2019]. Available from: https://www.ibm.com/downloads/cas/BBRQK3WY.

[5] Buterin VJwp, A Next-generation Smart Contract and Decentralized Application Platform, (2014).

[6] An overview of blockchain technology: architecture, consensus, and future trends, in: Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang (Eds.), Big Data (BigData Congress), 2017 IEEE International Congress on, IEEE, 2017.

[7] R.C. Merkle (Ed.), A Certified Digital Signature. Conference on the Theory and Application of Cryptology, Springer, 1989.

[8] M. Pilkington, 11 blockchain technology: principles and applications Research Handbook on Digital Transformations, (2016), p. 225.

[9] Architecture of the hyperledger blockchain fabric, in: C. Cachin (Ed.), Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.

[10] K.J. O'Dwyer, D. Malone, Bitcoin Mining and Its Energy Footprint, (2014).

[11] M. Castro, B. Liskov (Eds.), Practical Byzantine Fault Tolerance, OSDI, 1999.

[12] projects Tlf. Hyperledger [cited 19.03 2019]. Available from: https://www.hyperledger.org.

[13] S. King, N.S. Ppcoin, Peer-to-peer Crypto-currency With Proof-of-Stake, self-published paper, August (2012), p. 19.

[14] J.P. Anderson, Computer Security Technology Planning Study, ESD-TR-73-51 (1972).

[15] R. Courtney, W. Ware, Some informal comments about integrity and the integrity workshop, in: Z.G. Ruthberg, W.T. Polk (Eds.), Proc Of the Invitational Workshop on Data Integrity, National Institute of Standards and Technology, Special Publication, 1989.

[16] E. Coiera, Guide to Health Informatics, CRC press, 2015.

[17] Y. Levy, E. TJJIS, A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research, (2006), p. 9.

[18] M. Hölbl, M. Kompara, A. Kamišalić, L.J.S. Nemec Zlatolas, A Systematic Review of the Use of Blockchain in Healthcare, (2018), p. 470 10 (10).

[19] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.

[20] BlocHIE: a BLOCkchain-based platform for healthcare information Exchange, in: J. Shan, C. Jiannong, W. Hanqing, Y. Yanni, M. Mingyu, H. Jianfei (Eds.), 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 18-20 June 2018, Los Alamitos, CA, USA: IEEE Computer Society, 2018.

[21] A.S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P.S. Efraimidis, E. Kaldoudi, A blockchain-based notarization service for biomedical knowledge retrieval, Comput. Struct. Biotechnol. J. 16 (2018) 288–297.

[22] K. Peterson, R. Deeduvanu, P. Kanjamala, K. Boles, A Blockchain-Based Approach to Health Information Exchange Networks, (2017) 2017.

[23] D. Ichikawa, M. Kashiyama, T. Ueno, Tamper-resistant Mobile Health Using Blockchain Technology, ncbi.nlm.nih.gov (2017).

[24] V. Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Inf. J. (2018).

[25] J. Zhang, N. Xue, X. Huang, A secure system for pervasive social network-based healthcare, IEEE Access 4 (2016) 9239–9250.

[26] A. Roehrs, C.A. da Costa, R. da Rosa Righi, OmniPHR: a distributed architecture model to integrate personal health records, J. Biomed. Inform. 71 (2017) 70–81.

[27] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li (Eds.), Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications, Institute of Electrical and Electronics Engineers Inc, 2018.

[28] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain, J. Med. Syst. 42 (8) (2018).

[29] M.A. Rahman, M.S. Hossain, E. Hassanain, M. Rashid, S. Barnes, Spatial blockchain-based secure mass screening framework for children with dyslexia, IEEE Access (2018) 1-.

[30] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 6 (2018) 11676–11686.

[31] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.

[32] L. Zhou, L. Wang, S.Y. MIStore, A blockchain-based medical insurance storage system, J. Med. Syst. 42 (8) (2018).

[33] MedRec: using blockchain for medical data access and permission management, in: A. Azaria, A. Ekblaw, T. Vieira, A. Lippman (Eds.), 2016 2nd International Conference on Open and Big Data (OBD), 22-24 Aug 2016, Los Alamitos, CA, USA: IEEE Computer Society, 2016.

[34] A.F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, T. JMRS, V.H.C. de Albuquerque, A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform, Cogn. Syst. Res. 52 (2018) 1–11.

[35] H. Zhao, Y. Zhang, Y. Peng, R. Xu (Eds.), Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys, Institute of Electrical and Electronics Engineers Inc, 2017.

[36] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, MedBlock: efficient and secure medical data sharing via blockchain, J. Med. Syst. 42 (8) (2018).

[37] T. Mikula, R.H. Jacobsen, Identity and access management with blockchain in electronic healthcare records, 2018 21st Euromicro Conference on Digital System Design (DSD) (2018) 2018 29-31 Aug.

[38] Y.S. Hao Wang, Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain, (2018).

[39] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (7) (2018).

[40] J. Dias, L. Reis, H. Ferreira, Â. Martins, Blockchain for Access Control in e-Health Scenarios, arXiv preprint arXiv:180512267 (2018).

[41] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustain. Cities Soc. 39 (2018) 283–297.

[42] A blockchain application for medical information sharing, in: J. Chen, X. Ma, M. Du, Z. Wang (Eds.), 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE), 2018 30 March-1 April 2018.

[43] T. Bocek, B.B. Rodrigues, T. Strasser, B. Stiller (Eds.), Blockchains Everywhere – A Use-Case of Blockchains in the Pharma Supply-Chain, Institute of Electrical and Electronics Engineers Inc, 2017.

[44] F. Angeletti, I. Chatzigiannakis, A. Vitaletti, Privacy preserving data management in recruiting participants for digital clinical trials, Proceedings of the First International Workshop on Human-Centered Sensing, Networking, and Systems; Delft, Netherlands, ACM, 2017, pp. 7–12 3144733.

[45] S.A. Anastasia Theodouli, K. Moschou, K. Votis, D. Tzovaras, On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing, (2018).

[46] T. Nugent, D. Upton, M. Cimpoesu, Improving data transparency in clinical trials using blockchain smart contracts, F1000 Res. (2016) 5.

[47] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, et al., Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare, Oncotarget 9 (5) (2018) 5665–5690.

[48] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, J. Liu, S. Qing, D. Liu, C. Mitchell, L. Chen (Eds.), Towards Decentralized Accountability and Self-Sovereignty in Healthcare Systems, Springer Verlag, 2018, pp. 387–398.

[49] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-based data preservation system for medical data, J. Med. Syst. 42 (8) (2018).

[50] M. Laskowski, N. Osgood, D. Lee, R. Thomson, Y.R. Lin (Eds.), A Blockchain-Enabled Participatory Decision Support Framework, Springer Verlag, 2017, pp. 329–334.

[51] Y. Ji, J. Zhang, J. Ma, C. Yang, Y.X. BMPLS, Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, J. Med. Syst. 42 (8) (2018).

[52] X. Zhang, S. Poslad (Eds.), Blockchain Support for Flexible Queries With Granular Access Control to Electronic Medical Records (EMR), Institute of Electrical and Electronics Engineers Inc, 2018.

[53] Q. Xia, E.B. Sifah, A. Smahi, S. Amofa, X. Zhang, BBDS: Blockchain-based data sharing for electronic medical records in cloud environments, Inf. (Switzerland) 8 (2) (2017).

[54] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient centric agent: a block architecture, IEEE Access 6 (2018) 32700–32726.

[55] A decentralizing attribute-based signature for healthcare blockchain, in: Y. Sun, R. Zhang, X. Wang, K. Gao, L. Liu (Eds.), 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018 30 July-2 Aug. 2018.

[56] S. Rahmadika, K. Rhee, Blockchain technology for providing an architecture model of decentralized personal health information, Int. J. Eng. Bus. Manage. (2018).

[57] P. Zhang, J. White, D. Schmidt, G. Lenz, Applying Software Patterns to Address - Interoperability in Blockchain-based Healthcare Apps, arXiv preprint arXiv:170603700 (2017).

[58] W. Wilkowska, M. Ziefle, Privacy and data security in E-health: requirements from the user's perspective, Health Inf. J. 18 (3) (2012) 191–201.

[59] T.W. Bice, S.B. Boxerman, A quantitative measure of continuity of care, Med. Care 15 (4) (1977) 347–349.

[60] M. Raikwar, D. Gligoroski, K. Kralevska, SoK of used cryptography in blockchain, IEEE Access 7 (2019) 148550–148575.

[61] Frost & Sullivan, Global Blockchain Technology Market in the Healthcare Industry 2018–2022, (2019) 4847375.

1 Appendix A – Search strategy

The following search strategies were applied for respective database:

MEDLINE (via Ovid)
1 "block?chain*".ti,ab,kw.
2 (("bit?coin*" or "crypto?currenc*") adj2 technolog*).ti,ab,kw.
3 1 or 2

Embase (via Ovid)
1 "block?chain*".ti,ab,kw.
2 (("bit?coin*" or "crypto?currenc*") adj2 technolog*).ti,ab,kw.
3 or/1-2

Cochrane Library
#1 (block?chain*):ti,ab,kw (Word variations have been searched)
#2 ("bit?coin*" or "crypto?currenc*") near/2 technolog*:ti,ab,kw (Word variations have been searched)
#3 #1 or #2

Scopus
(TITLE-ABS-KEY (health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*)) AND (TITLE-ABS-KEY (blockchain*))

Google Scholar
health* | ehealth* | e-health* | "e health*" | medic* | clinic* | patient* | hospital* AND blochkhain*

Compendex (via Engineering Village)
found in Compendex for 1884-2019: ((((health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*) AND blockchain*) WN KY) OR (((health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*) AND blockchain*) WN CV))

Inspec (via Engineering Village)
in Inspec for 1896-2019: ((((health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*) AND blockchain*) WN FL) OR (((health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*) AND blockchain*) WN KY) (((health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*) AND blockchain*) WN FL))

ACM
(acmdlTitle:(health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*) OR recordAbstract:(health* OR ehealth* OR e-health* OR "e health*"

OR medic* OR clinic* OR patient* OR hospital*) OR keywords.author.keyword:(health* OR ehealth* OR e-health* OR "e health*" OR medic* OR clinic* OR patient* OR hospital*)) AND (acmdlTitle:(blockchain*) recordAbstract:(blockchain*) OR keywords.author.keyword:(blockchain*))

IEEE

(health* OR ehealth* OR e-health* OR medical OR medicine OR clinic* OR patient OR patients OR hospital OR hospitals) AND blockchain*

2 Appendix B – Protocol

Blockchain in healthcare and health sciences – a scoping review

1. Introduction

The technology of blockchain, with inherited characteristics such as decentralization, transparency and anonymization, currently reached its tip in the hype cycle with the value rally in Bitcoin and other cryptocurrencies during 2017. This hype in cryptocurrencies may have contributed blockchain to disrupt a range of data driven domains, including healthcare. The usage of blockchain has been proposed to improve many processes in health care and health science, from Electronic Health Records to Clinical Trial data management (Mettler 2016). Although blockchain in healthcare has been widely discussed in different forums in the last years, there is a little overview in the current literature of what has actually been developed and tested. To separate the hype from what has been empirically proven, this study aim to shed light and aggregate the results of published academic studies where blockchain has been utilized (or proposed to be utilized) to improve processes and services in the healthcare and health science domain. This literature review is to cover the research to date on blockchain implications within healthcare, health science and health education.

1.1 What is blockchain

Blockchain allows mutually distrusting entities to interact without the presence of a central trusted third party. It can be considered as a database that maintains a continuously growing set of data records where the data records can be represent as blocks of a chain. These data records/blocks are: readable by all participants, writable by all, and tamper-proof by all. Due to these properties, blockchain has gained much attention for various applications. Bitcoin is the first application of blockchain proposed by Satoshi Nakamoto in 2008 (Nakamoto 2008). Bitcoin is also known as a "cryptocurrency". It allows a purely peer-to-peer version of electronic cash where online payments are sent directly from one party to another without going through a financial institution.

Since bitcoin, many different applications of the blockchain concept have emerged such as finance/banking (Peters and Panayi 2016), Internet-of-Things (Conoscenti, Vetro et al. 2016), healthcare (Griggs, Ossipova et al. 2018), supply chain management (Tian 2016), government (Ølnes, Ubacht et al. 2017), voting (Wright and De Filippi 2015), energy management (Aitzhan and Svetinovic 2018) and real estate (Spielman 2016). Bitcoin remains the largest blockchain to this date, although many other blockchains have been introduced since the birth of Bitcoin, both new cryptocurrencies and other applications besides digital currencies (Swan 2015).

Blockchain, in its original form, can further be described as a decentralized digital ledger in a peer-to-peer network, supported by sophisticated cryptography and relied on a consensus mechanism (Nakamoto 2008). This for instance allows decentralized transactions and data management. Blockchain also allows for smart contracts. The blockchain Ethereum is at this date the largest facilitator of smart-contracts on a blockchain (Vitalik 2014).

1.2. Health information systems and health systems

Health Informatics deal with the use of information and communication technologies to re-imagine, refactor, re-engineer and energize knowledge-based, people-centered care delivery systems. To fulfil these particular purposes, Health information systems (HIS) must support the work of individuals, institutions as well as of policy makers. From the perspective of citizens, health information systems must aid in their confidential sharing of information about health problems, the analysis and explanation of health problems by knowledgeable clinicians and the organization, delivery and assessment of knowledge-based care. From the perspective of health professionals, health information systems must support the recording and analysis of information about health problems, individual and collaborative health problem-solving, clinical decision-making, referral and ordering. From the perspective of health institutions and policy-makers, health information systems must fulfil legal requirements such as the creation of non-mutable recordings of healthcare events, protection of recordings that already have been created and the proper use of health information to achieve the purposes of the particular institution.

As of 2018, a shift in citizens' expectations, the commoditization of biomedical knowledge, the Internet of Things (IoT)- facilitated health data sharing and the virtualisation of caregiving itself commands a major rethinking and reorganisation in healthcare and health information system design. Blockchain technology may have the potential to contribute in this rethinking and reorganisation. With some of its key attributes; security, anonymity and data integrity without any necessary third party government, blockchain technology posses many appealing characteristics that could be utilized in this field.

1.3 Research impact

Blockchain in healthcare and health science as a research area appears to be increasing. In the current literature, few publications are published before 2016. From 2016 and onwards, there are several blockchain research projects that aim to investigate how the technology best could be utilized in healthcare. Of those, the majority are of an opinion or editorial character.

There seems to be a lack of a systematic review that summarizes published research on blockchain applications within the health domain. To summarize what we already know about the technical solutions, implementation possibilities and potential barriers, there is a need to seperate actual knowledge from non-empirical opinions that have bursted out in the wake of the blockchain hype. A systematic review is also needed to propose directions for future research within the broad topic: Blockchain within healthcare and health science.

2. Aim and Objectives

The aim of the study is:

1. To obtain a systematic overview of scientific studies which propose blockchain technology to improve processes or services in healthcare, health sciences and health education.

Secondary objectives:

1. To present an overview of what specific systems, processes and challenges within the health domain that currently are being addressed by blockchain technology.
2. To systematically review scientific evidence on the effects of architectures building upon blockchain infrastructure in order to improve trust and transparency within the health domain.
3. To summarize the technical solutions that are categorized as "blockchain" and their key attributes for the health domain applications.

2.1 Review questions

The main questions of this review are as follow:

1. What scientific literature exists on the usage and development of blockchain technology with the aim to solve/improve challenges within the health domain?
2. What systems, processes and challenges within the health domain are targeted with blockchain enhanced solutions?
3. What are the technical specifics for blockchain applications aimed for the health domain in the current peer-reviewed literature?

3. Method

The methodology for this scoping literature review follow the recommended outline of Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher, Shamseer et al. 2015).

The scoping literature review targets only published academic research in scholarly journals, conference proceedings and workshop reports that asses blockchain concepts in the healthcare, health science and health education domain.

3.1 Eligibility (inclusion) criteria

Studies that fulfill all of the following criteria's are to be included:

1. Studies that propose a blockchain solution that addresses a problem in healthcare, health science or health education that has a clear evaluation of the solution presented.
2. Describes the technical blockchain architecture of the application, including what type of blockchain it is relied on (existing blockchain, new blockchain) with technical details that describes the blockchain (mining technique, data storage, hash functions and consensus mechanisms).
3. Describes an implementation strategy OR consider implementation challenges.

Table 1. Inclusion criteria

Inclusion criteria	**Outcome**	
	Yes	No
Proposal of blockchain solution that is evaluated		
Technical description of the blockchain architecture (including at least 4 out of the 9 technical variables listed under Variables.)		
The problem addressed is in the health domain		
Assessment	**In**	**Out**
Tick		

Further instructions for inclusion:

For the purpose of this review, the definition of blockchain will rely on the authors definition of blockchain - If the concept or application are label as blockchain by the authors in the published material, it should be included (provided the other inclusion criteria's also are meet)

3.2 Exclusion criteria:

Studies which meet one or more of the following criteria are to be excluded:

1. Lack sufficient architectural description (mining technique, data storage, hash functions and consensus mechanisms).
2. Lack of real world implementation considerations.
3. Discussion, commentary or editorial papers that not propose any real developed concept.
4. Language other than English and not translatable by Google Translate.

3.3 Search strategy

To identify relevant research, we will search in medicine and health related databases (MEDLINE, Embase, The Cochrane Library (Cochrane Database of Systematic Reviews (CDRS), the Cochrane Central Register of Controlled Trials (CENTRAL)), engineering and informatics databases (ACM, IEEE, INSPECT) and interdisciplinary databases (Web of Science, SCOPUS). We will search for grey literature in Google Scholar.

We will apply a combination of thesaurus (when available) and free-text terms optimized to identify studies examining the use of blockchains within healthcare. To identify potentially relevant studies not covered in the included databases we will also screen bibliographic citations in the included studies and review articles. The searches will not be restricted by date and no language restrictions will be applied.

The search will target published research in scholarly journals, conference proceedings and workshop reports that asses blockchain concepts in the healthcare, health science and health education domain.

3.4 Quality assessment

As an important part of the review process a meticulous quality assessment of included publications were conducted by several of the reviewers

3.5 Data management

Abstracts will be made available to the reviewer by importing the search query result into Nvivo and EndNote x8. The search query result will also be downloaded as a .csv document and converted to a Google spreadsheet document. The spreadsheet will be used to label publications that fulfil the inclusion criteria.

3.6 Selection process

Two reviewers will screen the titles and abstracts against the inclusion criteria independently. Full-text versions of selected studies will then be reviewed to confirm whether or not the study should be included in the final review, done by both reviewers independently. If the two reviewers disagree on the inclusion of a study, a third reviewer will assist in the decision making.

3.7 Data collection process

One of the reviewers will collect data by reading full-text versions of the studies and plot the values directly into a spreadsheet and highlight key statements in the text using tools in Nvivo.

3.8 Data items to be extracted

List of variables:

The following data will be extracted from the selected studies:

Meta data:

1. Name of first author,
2. Year of publication,
3. Study design,
4. Study setting,
5. Geographical area of the study,

Implementation variables:

6. Topic within the health domain that is addressed,
7. Technical problem which the solution is aimed to improve,
8. Requirements for solving the problem,
9. Main implementation challenges,
10. Legal/regulatory issues,
11. Other mentioned barriers,

Technical variables:

12. Type of blockchain (private, public or consortium),
13. Existing or new blockchain,
14. Mining technique and incentive mechanism,
15. Data storage design,

16. Consensus mechanism,
17. Hash function used
18. Scalability
19. Energy consumption
20. Infrastructure dependencies

3.9 Data synthesis

The extracted data will be summarized in tables and a narrative review will be prepared. Based on an initial search and the fact that blockchain in healthcare is a new research area, we expect to find a limited number of studies to include in this review. Due to the cross-sectional nature of blockchain in healthcare research and the limited restrictions on study type in this review, we also expect to include a wide range of study designs, it can therefore be difficult to quantify the extracted data in numerical terms. Hence, emphasis will insteed be on the narrative review. For the same reason, a meta-analysis will most likely not be feasible at this point.

4. Ethical considerations

Since this study is a systematic literature review, covering articles and conference proceedings in peer reviewed journals, no ethical problems should be related to the research. No measures are to be taken regarding ethical consideration.

5. References

1. Conoscenti, M., et al. (2016). Blockchain for the Internet of Things: A systematic literature review. Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of, IEEE
2. Higgins, J. P. and D. G. Altman (2008). "Assessing risk of bias in included studies." Cochrane handbook for systematic reviews of interventions: Cochrane book series: 187-241
3. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on, IEEE.
4. Moher, D., et al. (2015). "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement." Systematic Reviews**4**(1): 1
5. N. Satoshi (2008), Bitcoin: A Peer-to-Peer Electronic Cash System,

[Online]. Available: https://bitcoin.org/bitcoin.pdf

6. Peters, G. W. and E. Panayi (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Banking Beyond Banks and Money, Springer**:** 239-278.
7. Spielman, A. (2016). Blockchain: digitally rebuilding the real estate industry, Massachusetts Institute of Technology.
8. Swan, M. (2015). Blockchain: Blueprint for a new economy, " O'Reilly Media, Inc."
9. Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. Service Systems and Service Management (ICSSSM), 2016 13th International Conference on, IEEE
10. Buterin, V., *A next-generation smart contract and decentralized application platform.*white paper, 2014.
11. Williams-Grut, O. (2016). "Estonia is using the technology behind bitcoin to secure 1 million health records." Bus Insid.
12. Wright, A. and P. De Filippi (2015). "Decentralized blockchain technology and the rise of lex cryptographia."
13. Ølnes, S., et al. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, Elsevier.

B

Hasselgren, A., Rensaa, J.A.H., Kralevska, K., Gligoroski, D. and Faxvaag, A., 2021. Blockchain for increased trust in virtual health care: proof-of-concept study. Journal of Medical Internet Research, 23(7), p.e28496.

Original Paper

Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study

Anton Hasselgren[1], MSc; Jens-Andreas Hanssen Rensaa[2], MSc; Katina Kralevska[2], PhD; Danilo Gligoroski[2], PhD; Arild Faxvaag[1], MD, PhD

[1]Department of Neuromedicine and Movement Science, Norwegian University of Science and Technology, Trondheim, Norway

[2]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim, Norway

Corresponding Author:
Anton Hasselgren, MSc
Department of Neuromedicine and Movement Science
Norwegian University of Science and Technology
Mellomila 71
Trondheim
Norway
Phone: 47 46948498
Email: anton.hasselgren@ntnu.no

Abstract

Background: Health care systems are currently undergoing a digital transformation that has been primarily triggered by emerging technologies, such as artificial intelligence, the Internet of Things, 5G, blockchain, and the digital representation of patients using (mobile) sensor devices. One of the results of this transformation is the gradual virtualization of care. Irrespective of the care environment, trust between caregivers and patients is essential for achieving favorable health outcomes. Given the many breaches of information security and patient safety, today's health information system portfolios do not suffice as infrastructure for establishing and maintaining trust in virtual care environments.

Objective: This study aims to establish a theoretical foundation for a complex health care system intervention that aims to exploit a cryptographically secured infrastructure for establishing and maintaining trust in virtualized care environments and, based on this theoretical foundation, present a proof of concept that fulfills the necessary requirements.

Methods: This work applies the following framework for the design and evaluation of complex intervention research within health care: a review of the literature and expert consultation for technology forecasting. A proof of concept was developed by following the principles of design science and requirements engineering.

Results: This study determined and defined the crucial functional and nonfunctional requirements and principles for enhancing trust between caregivers and patients within a virtualized health care environment. The cornerstone of our architecture is an approach that uses blockchain technology. The proposed decentralized system offers an innovative governance structure for a novel trust model. The presented theoretical design principles are supported by a concrete implementation of an Ethereum-based platform called VerifyMed.

Conclusions: A service for enhancing trust in a virtualized health care environment that is built on a public blockchain has a high fit for purpose in Healthcare 4.0.

(J Med Internet Res 2021;23(7):e28496) doi: 10.2196/28496

KEYWORDS

blockchain; ethereum; decentralization; Healthcare 4.0; virtualization; trust

Introduction

Overview

As a result of health care development, societies are undergoing a current demographic shift—people live longer, and fewer are born. The overall increase in life expectancy between 1970 and 2013 was 10.4 years on average for Organization for Economic Cooperation and Development countries [1]. A direct effect of this demographic shift [2,3] is that noncommunicable and chronic diseases become more prevalent, which presents a substantial socioeconomic challenge. Consequently, fewer caregivers need to support an ever–increasing number of retirees with a rising number of chronic diseases. This unsustainable scenario is the strongest motivation behind many different ongoing proposals for transformations in the health care industry. Delivering health care, as we know it today, will most likely be unaffordable for any health system in 15 years from now, and many health services will have to be delivered by nonprofessionals and machines. This includes artificial intelligence health workers and devices connected via machine-to-machine protocols and automated, computerized services, which will be accessible via fast connections from anywhere, anyhow, and at any time (5G).

Furthermore, individuals will be forced to take more responsibility for their own health, take preventative measures, seek proper care in a timely manner, and behave more like autonomous patients. To facilitate this, there is a need to provide the right tools to encourage and enforce this transformation, both from the delivery side (health care providers) and the receiver side (patients). This transformation toward Healthcare 4.0 will challenge many of the present key components in a functional health system, where the concept of trust is one.

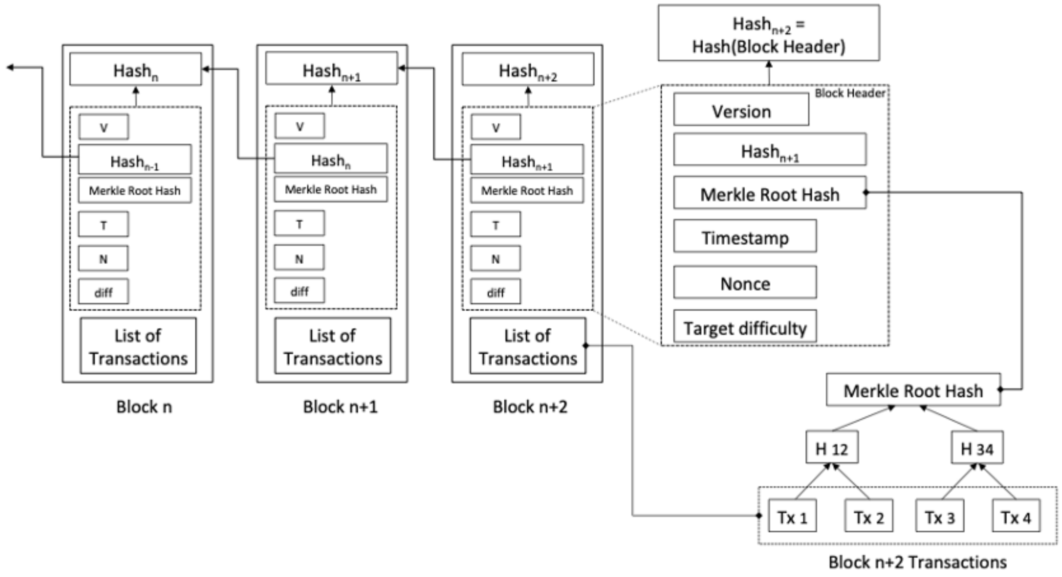
The first contribution of this paper is to review and predict the evolution of health care, and to identify the potential problems that could emerge in this transformation. It forms a theoretical foundation and urges the need for novel solutions to enhance trust. Second, the presented theoretical design principles are supported by the concrete implementation of a proof of concept. For this contribution, we choose the cornerstone in our architecture to be a blockchain technology implemented as an Ethereum-based platform called VerifyMed.

The remainder of this paper is organized as follows: the first section introduces blockchain and previous related work; the next section presents the method applied in this work; the following section outlines the results of technology forecasting and presents a trust issue in a virtualized health care environment; *the next* section presents a novel blockchain-based trust model for competence verification of health care personnel, and the final section provides a discussion and conclusions of the work.

Related Work and Blockchain Overview

Blockchain can be seen as an unconventional platform that alleviates the reliance on a single, centralized authority, yet it still supports secure and pseudoanonymous (or anonymous) transactions and agreements directly between interacting parties. It offers various degrees of decentralization, immutability, and consensus firmly founded in the mathematical principles of modern cryptography. A blockchain can also be described as an immutable ledger that logs data entries in a decentralized manner. In its original form, a blockchain enables entities to interact without a central trusted third party. The blockchain consists of a continuously growing set of data entries bundled together into blocks of data (Figure 1). Upon acceptance of the blockchain, these blocks are linked to the previous and future blocks sequentially [4]. In blockchain's original definition, this ledger of data blocks is decentralized and distributed across many nodes. This distributed ledger is transparent, verifiable by all, and tamper-proof. Owing to these properties, the blockchain has gained much attention for various applications. The first use case of a blockchain, Bitcoin, was introduced by a person or a group under the name of Satoshi Nakamoto in 2008 [5]. Bitcoin is also known as *a cryptocurrency.* Although cryptocurrencies remain the primary use case for blockchain, there is a substantial interest in applying this technology for other purposes and sectors [6]. Additionally, a blockchain allows for smart contracts—self-execution contracts that do not require any central authority. The use cases of blockchain in the health domain are increasing exponentially, as shown by Hasselgren et al [7], among others.

Figure 1. A generic overview of a blockchain structure.



Blockchain technology has five fundamental attributes that define the technology: (1) distribution, (2) decentralization, (3) time stamping, (4) data provenance, and (5) nonrepudiation. These five attributes are applied when addressing the fundamental problems in health care informatics and are part of driving the transformation toward Healthcare 4.0. The first generation of blockchain platforms led by Bitcoin [5] had a specially defined programming language for users to construct different transactions in the blockchain. The initial design rationale was that the programming language should be as simple as possible to satisfy the needs for building various transaction types and should not be a fully developed and powerful programming language. In computer science, the category of powerful programming languages is called the *Turing Complete*. The first blockchain platform that offered a Turing Complete language for programming, not just simple transactions but also more complex *smart contracts* and fully developed apps, was Ethereum [8]. There is an active debate on which concept is better and safer—development of malicious programs for blockchain platforms that do not have the Turing Complete programming language is very difficult and limited, in contrast to blockchain platforms that have the Turing Complete languages [5,9]. Nevertheless, it seems that the blockchain platforms that come with a fully developed Turing Complete programming language are very suitable for developing decentralized applications (dApps) for Healthcare 4.0, which is further elaborated in the next section.

Blockchain Platforms, dApps, and Smart Contracts

There are several decentralized platforms and frameworks for building dApps. Ethereum is the most common in health care applications [10]. This is most likely due to the large number of developers in the Ethereum community. Nevertheless, Ethereum has proven to be a solid platform for health care dApps [11]. Compared with the first and largest blockchain to date—Bitcoin—Ethereum has incorporated smart contracts, a function that substantially opens up the features of dApps built on Ethereum.

Smart contracts can be considered as self-executing contractual agreements, where preagreed upon provisions are formalized in the source code. Smart contracts can be automatically enforced based on these preagreed provisions, and they can work without any third party. The functions within a smart contract can be awoken in a blockchain transaction, and the use of this functionality could appeal to the health domain [8].

Zhang et al [11] stated that a well-designed health care dApp should limit the storage of encrypted sensitive data on the blockchain. Furthermore, they recommend that a dApp dealing with health care data should support Turing completeness to facilitate communication among various parties and handle the exchange of sensitive patient data. In the study by Kuo et al [10], there were clear indications that Ethereum, Hyperledger, and Multichain are more suitable platforms for the health domain than other blockchains.

Blockcerts [12] is a standard developed for verifying certificates of competence by storing signatures on a blockchain. The standard relies on existing trust relationships between the issuer and verifier of the certificate. Baldi et al [13] showed that certificates within this system could be spoofed. They also proposed the use of decentralized identifiers to govern such certificates. At present, there are private initiatives for medical credentials that use a blockchain. The first on the market was ProCredEx by Hashed Health [14]. They state that they have developed a blockchain-based solution that enables faster onboarding and credential verification.

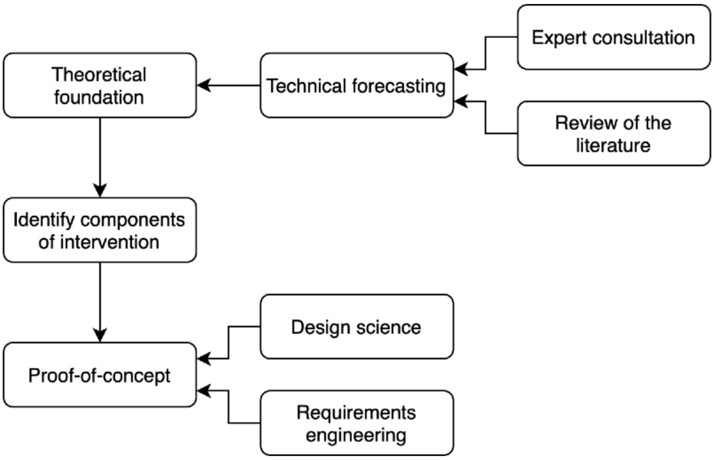
Furthermore, a newly introduced collaborative project between Axuall, Inc and Metro-Health [15] announced a service for credentials of clinical practitioners. They state that they will enable digital portfolios that will include documentation of a practitioner’s education, specialty training and board certifications, licenses, sanctions or medical malpractice judgments, evaluations, work history, and hospital affiliations. As these are private endorsers, there is no published peer-reviewed literature on their technical solutions. In addition to what is mentioned above, based on our knowledge, there is no published research that has addressed the same scope as our framework. As described earlier, several private organizations have created solutions for medical credentials by using blockchain technology. However, these are all based on the United States and are somewhat tailored to the US health system. We explore a broader solution in the form of a decentralized trust model that addresses the current issues with board certificates and credentials and creates an immutable portfolio of completed clinical work by a health care professional that is verifiable by all. The research approach used in this study is described in the following section.

Methods

Overview

The research approach used in this study, as shown in Figure 2, follows one of the frameworks presented by Campbell et al [16], which describes a framework for the design and evaluation of complex intervention research within health care. Our study aims to address the following two key issues outlined in the framework: (1) establish the theoretical basis of the intervention and (2) identify and describe the components of the complex intervention.

Figure 2. Research approach for the presented work.



Summary of Knowledge and Technology Forecasting

We applied the most common method for addressing technology forecasting by reviewing the current literature and consulting domain experts [17]. The domain expert consultation was conducted in an unstructured manner; a convenient sample of (health) informatics experts from Norway was consulted about their views on the future of health care and Healthcare 4.0. A scoping review of the literature on the future of health care was performed in a semisystematic manner, and this is described in the section *Summary of Knowledge: Healthcare 4.0*.

Identifying Components of the Intervention

On the basis of the forecasting of Healthcare 4.0, a potential trust challenge is described and elaborated as the primary component of the intervention. This is presented in section *Trust in Healthcare 4.0*.

Proof of Concept

Furthermore, our work presents some technical components of a proof of concept to conceptualize (1) and (2), following the principles of design science [18] and requirements engineering [19]. This is presented in the section *VerifyMed: A Novel Trust Model*.

Results

Overview

We first describe a technology forecast of health care and then demonstrate how trust will emerge in this transformed health care system as a component of an intervention. The proof-of-concept VerifyMed is presented in a separate section, that is, *VerifyMed: A Novel Trust Model*.

Summary of Knowledge: Healthcare 4.0

Healthcare 4.0 [20] is a strategic concept for the health domain derived from the Industry 4.0 concept. The aim of Healthcare 4.0 is to allow for advanced virtualization to enable the personalization of health care in real time for patients, professionals, informal health workers, and nonhuman health workers. A transformation toward Healthcare 4.0 will be a shift from hospital or professional-centered health care (patient in hospitals) to a globalized, virtualized, and self-administered health care via distributed patient-centric care (multiple care providers) and later to patient-driven care fueled by personally generated health data.

Lasi et al [21] define Industry 4.0 with a wide range of current concepts: smart factories, cyber-physical systems, self-organization, new systems in distribution and procurement, new systems in the development of products and services, adaptation to human needs, and corporate social responsibility. Similarly, this categorization has been applied to health system development in the Healthcare 4.0 concept.

Thuemmler and Bai [20] state that:

> *The aim of Healthcare 4.0 is to allow for progressive virtualization in order to enable the personalization of healthcare next to real-time for patients, professionals, and formal and informal caregivers. The personalizing of healthcare will be achieved through the massive use of cyber-physical systems, cloud/edge computing, the Internet of everything including things, services and people and evolving mobile communication networks (5G).*

The six design principles from Industry 4.0 could be applied to Healthcare 4.0 to forecast health care transformation and to design applications with a high fit for purpose. The following design principles were proposed [22]:

1. Interoperability: enable people and machines to communicate through data standards and standardized infrastructure.
2. Virtualization: technologies for interoperability, faster internet connections, and connected devices enable the movement of parts of the physical processes in health care to a virtual environment.
3. Decentralization: linking real-time data and users together opens up more autonomous decisions and reduces the necessity of centralized services.
4. Real-time capability: a higher proportion of connected devices and people enables changes in real time.

5. Service orientation: a shift from products to services based on accumulating data could adapt faster to market changes.
6. Modularity: a higher degree of module-based delivery and configuration enables faster adoption of changing needs.

From an academic perspective, design principles are the foundation of the design theory [23]. As outlined in the section *Proof of Concept*, the design theory method is followed in developing our proof-of-concept platform, VerifyMed.

The following section presents an emerging problem in Healthcare 4.0, which serves as the basis for the components of our intervention.

Trust in Healthcare 4.0

Overview

The definition of trust is a broad, multilayered, and complex concept that varies depending on the academic discipline that uses the term [24]. For this study, we have adopted the following broad definition of trust: *a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another* [25].

Trust From a Human Psychology Perspective

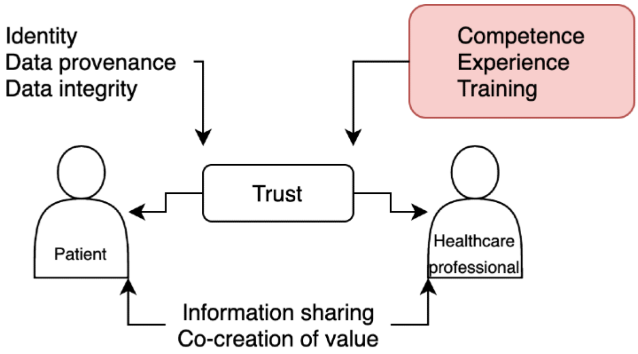
A central part of clinical practice is trust between a patient and a health care professional [26]. Maintaining trust with patients is a core function for physicians in their clinical practice [27]. The General Medical Council states "patients must be able to trust doctors with their lives and health" [28]. This is also a part of the obligations of other health care professionals such as nurses [29]. Trust in health care professionals is considered a foundation for effective service delivery [30] and a core attribute in patient-centered care [31].

Commonly, trust is divided into interpersonal, social, and dispositional trust [32].

Furthermore, trust between a trustor and a trustee is encouraged by the trustee's reliability (good reputation), competence (having skills to perform the task at hand), and integrity (honesty) [33]. Trust in a physician is related to increased treatment adherence, patient satisfaction, and improved health status [34]. Patients most commonly base their trust on doctor's characteristics such as competence, compassion, privacy and confidentiality, reliability and dependability, and communication skills [35].

We know from other industries that a successful web-based consultation in health care delivery service requires a value cocreation between the caregiver and the patient [36]. Caregivers need active participation from patients to benefit from this cocreation. Several factors contribute to the trust foundation, which is the basis for value creation, as illustrated in Figure 3. Our approach targets the verification of competence, experience, and training (highlighted in Figure 3).

Figure 3. Factors influencing trust in a patient-caregiver interaction.



Trust in Medical Technologies

When trusting medical technologies, institutional trust and technical reliability are deeply intertwined [37]. A key takeaway when reviewing Industry 4.0 is the need to explore further and understand how to build trust in the context of digital and virtualized health. This is related to trust in systems and information (human system) and people having the control of sharing information (human-human through the system).

Trust Issues in Healthcare 4.0

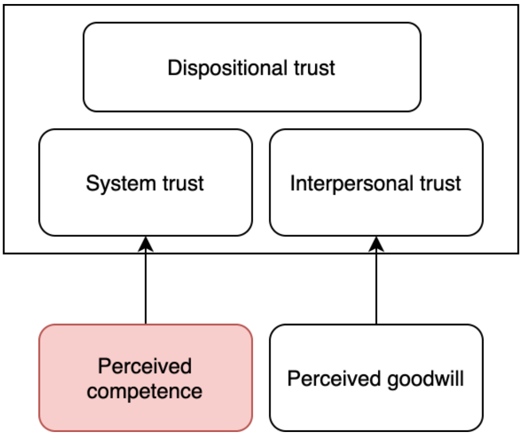
To conceptualize one part of the trust ecosystem in health care, we present the following theoretical issues with trust in a virtual patient-caregiver relationship: the patient needs to trust that the caregiver has the right competence (and authority) to deal with his or her health problem in a physical as well as in a virtualized health care environment. The caregiver needs to show the patient that he or she possesses the right competence to deal with the health problem of that specific patient; otherwise, the patient will possibly go somewhere else.

There are currently few or no systematic and objective tools to verify the competence and experience of health professionals in a transparent and accessible manner. The records of cases of delivered care are often stored in the electronic health record of the respective hospital. If a health care worker changes an employer, there is little or no opportunity to bring the ledger of given care (work experience). Like other industries, the health care industry has experienced a fast turnover of personnel. More health care workers change employers at a faster rate [38]. More health care workers are also moving across borders and jurisdictions at an increasingly higher pace [39]. In these cases, a tamper-proof, accessible record of the work history of someone as a health care professional, owned and controlled by no single entity, could be valuable. If this *portfolio* was stored in a decentralized manner, easily accessible with the consent of the particular health care worker, onboarding processes for employers in the health care domain could be improved and that the health care worker could feel confident in that they control their own reputation by providing evidence-based care that could be verified at any time.

There is a need for patients, health care workers, and health care facilities to be able to verify the skill, competence, and formal certificates of health care personnel, especially when health care is moving toward Healthcare 4.0. Furthermore, it is essential to create an audit trail of complete work for health care workers; this could function as a portfolio that could potentially be used for future employers, freelance work, and increased confidence among health care workers.

Previous work has concluded that perceived competence and perceived goodwill are contributing factors to the system and interpersonal trust [24,32]. In a virtualized health care environment, it becomes increasingly important to verify the competence and credentials of health care professionals, as perceived competence is an essential component in building trust [40,41]. This highlighted component of perceived competence in Figure 4 is one part that the concept of VerifyMed partially addresses.

Figure 4. Trust model (adapted from Leimeister et al [32]).



The following section presents a proof of concept that addresses those needs.

VerifyMed: A Novel Trust Model

Overview

Our proposed architecture's technical core and the operational functionality are described in the studies by Rensaa et al [42-44]. In addition to that technical part, we describe some of the crucial functional and nonfunctional requirements and the principles that influenced our design rationale.

Our proposed architecture provides a solution for enhancing trust between a caregiver and a patient within a virtualized health care environment. The cornerstone feature in our architecture is its ability to capture trust relationships within the health care system and put them in a blockchain. Patients can use this trust mechanism to confirm credentials and potentially enhance trust in a caregiver during their interaction. Furthermore, the architecture includes tools for evaluating these interactions publicly on a blockchain. These evaluations served as a file for the caregiver's experience. We proposed the following three types of evidence for building trust in a virtualized health care environment: evidence of authority, evidence of experience, and evidence of competence [43].

The functional requirements describe the key features that we desire in our system based on our problem statement. Nonfunctional requirements describe the properties of the system, such as security, privacy, and performance requirements. Nonfunctional requirements often have a sizable architectural impact on how the system is implemented, whereas the functional requirements present the functionality that should be present within the architecture. These requirements are deduced from both industry requirements for handling patient data and the perceived problems deduced from our problem statement.

Previous research on blockchain apps within the health care industry has defined general principles for the requirements and system design principles that should be followed. Zhang et al [11] defined the metrics for evaluating blockchain apps within the health care industry. Although they are primarily directed toward the American Health Insurance Portability and Accountability Act (HIPAA), we generalize and try to capture some of these principles in our requirements.

Regulatory Compliance: Compliance With Current Health Data Laws and (Health) Privacy Regulations

Several regulatory bodies are responsible for preserving privacy and access rights to personal health data. The most prominent are the HIPAA for the United States and the General Data Protection Regulation (GDPR) for the European Union. In addition, most countries have national health data laws that further regulate health data for their citizens. In the scope of this study, we explored the GDPR compliance for VerifyMed. There are currently some uncertainties around general blockchain compliance with the GDPR [44], and these uncertainties, mainly around the level of anonymization and identification of data controllers in a decentralized network, have not yet been clarified in any court case by the European Data Protection Board. However, it has been argued that there are no compliant blockchains, only complaint use cases, and apps [44]. The VerifyMed platform is designed to enhance user privacy and access control, and the following relevant GDPR articles have been addressed [45].

The VerifyMed platform is also designed to enhance the right of access by the data subject (Article 15 of the GDPR). As the system is designed not to store any personal data on the blockchain, it is also compliant with Article 17 of the GDPR (right to erasure or "right to be forgotten"), which only refers to personal data.

As the system is decentralized by design and there are possibilities for the user to access and receive the data at any time, it is compliant with Article 20 of the GDPR (right to data portability). The system requires an identity management solution to ensure full anonymization of the users and complies with Article 32 of the GDPR (security of processing). Identity management is not addressed within the scope of this study.

Key Functional Requirements

In accordance with the patient-centric health care system, we chose to define our main functional requirements in the context of the patient. As will be described later, the blockchain component of our architecture can be defined as a provider-centered model. We also note that fulfilling our patient-centered requirements allows the architecture to be used in settings outside of the patient and caregiver relationship. The main purpose of the model was to serve a patient-centered use case. The key patient-centered functional requirements were as follows:

1. Verification of caregiver credentials: a patient using a third-party system to talk with a caregiver should be able to verify the credentials by only using data from the blockchain. The patient must be able to do so without relying on any trust in the medical professional.
2. Verification of caregiver experience: a patient should be able to evaluate the experience of a medical professional by looking at data from the blockchain. Thus, the credibility of the data on blockchain must be enforced. The presented patient-centered requirements trigger opinionated system design choices to support this functionality. We additionally define two key features and refer to them as other deduced requirements. Therefore, these features will be subject to further specifications through nonfunctional requirements.
3. Transparency of blockchain data: to support data transparency to patients, we chose to use a publicly available blockchain to store the blockchain data. As these blockchains often have an associated fee with transactions, the system must take this into account.
4. Governance of blockchain data: to ensure that the trust relationships on the blockchain are anchored in the real world, they should be anchored in the existing corresponding trust relationships within the health care system. Just as there are governance entities responsible for credentials in the real world, they should be present in the proposed architecture as well.

Nonfunctional Requirements (via Quality Attributes)

Overview

In addition to the functional requirements above, we also surface the nonfunctional attributes of the system through quality attributes. The number of quality attributes of a system is unbounded. Therefore, this section presents the quality attributes that are considered to have the most significant architectural impact on the system.

Security Requirements

Fraudulent Treatments

A treatment cannot be published in the blockchain by unauthorized parties. All treatments must be cryptographically protected by an entity with direct or implicit authority to publish treatments.

Fraudulent Treatment Approvals

A treatment cannot be approved on the blockchain by unauthorized parties. All treatments must be approved by a license holder who the patient approves.

Fraudulent Evaluation

It should be impossible to publish an evaluation without going through a valid treatment. Once treatment has a related patient-reported outcome measure (PROM) published, it should not be possible to create another PROM related to the same treatment.

The Integrity of Treatments

It must be possible to ensure that a treatment or evaluation has not been tampered after their publication to ensure the credibility of these data sets. It is possible to prove this by using blockchain data.

Privacy Requirements

Unlinkability to Patients

The identity of patients must be treated as confidential. It should not be possible to link a transaction on the blockchain to a specific patient without any further knowledge from outside the blockchain. This will contribute to making the proposed system GDPR and HIPAA compliant (reference to regulatory compliance).

The Anonymity of Patients

The content of evaluations and treatments published on the blockchain should not reveal the identity of patients. The data published on the blockchain should either be a summary that cannot be linked to the patient or in another format that cannot be linked to a specific patient.

Access to Patient Data

The complete evaluations, including data linkable to patients, should be stored outside the blockchain. These data sets should be used to control patients. Access to these data sets for entities outside the patient and caregiver interaction should be denied unless the patient grants access.

Availability Requirements

Addition of New Governance Entities

It should be possible to add new governance entities dynamically without any code changes to the original contracts on the blockchain.

Recoverability After Authority Loss

If a governance entity becomes permanently unavailable or misbehaves, it should be possible to remove it, that is, to recover the dApp into a healthy state without interaction from the misbehaving authorizing entity.

Scalability Requirements

The amount of data on the blockchain should be minimal: the public blockchain is an expensive storage medium. Small data formats and encoding should be used to represent the data in the blockchain.

Performance Requirements

Minimization of transactions: interactivity with the blockchain should be reduced. The number of transactions required to go from the start to the published PROM should be small.

The Architecture

Overview

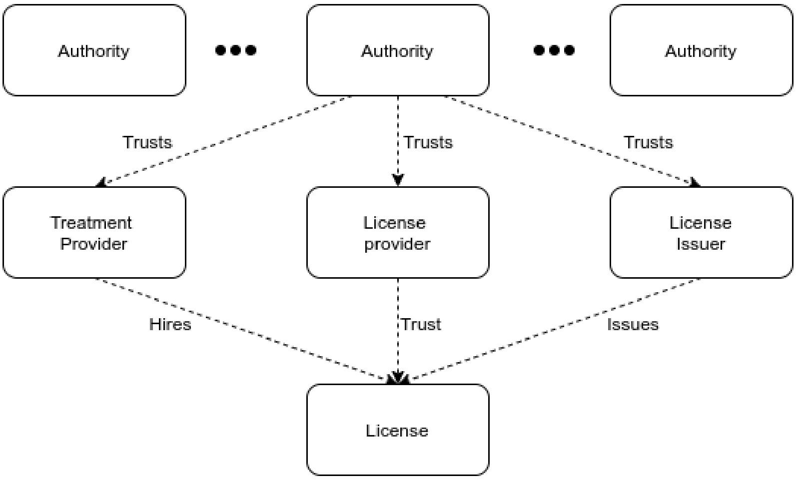
Our novel architecture provides trust between caregivers and patients within a virtualized health care environment. This is done through three main processes: evidence of authority, evidence of experience, and evidence of competence, each with its own components and stakeholders associated with them. We first define the terminology used in our architecture. Second, we present our proposition through an overall reference architecture. Finally, we describe how we further refine the reference architecture. We do this by describing the processes in the order in which they occur in the real world, along with the main components associated with them.

Terminology

Our architecture uses a concept for many different stakeholders, each represented by a given terminology. The stakeholders shown in Figure 5 are defined as follows:

1. Authorities: these are top-level government actors that have the overall responsibility of the health care sector (eg, national health directorates).
2. License: a license represents the practitioner's role as health personnel. Although a license in a traditional sense is the authorization of health personnel, we instead use it to represent the personnel themselves. Authorization is captured through trust relationships related to licenses.
3. License issuer: organizations that issue licenses for health personnel. License issuers are the only ones that can create licenses.
4. License provider: organizations that give formal authorization to practice for a license.
5. Treatment provider: organizations in which practitioners operate and are responsible for issuing treatments for patients. Examples include hospitals, clinics, and virtualized health care services.

Figure 5. Trust relationships published on the blockchain.

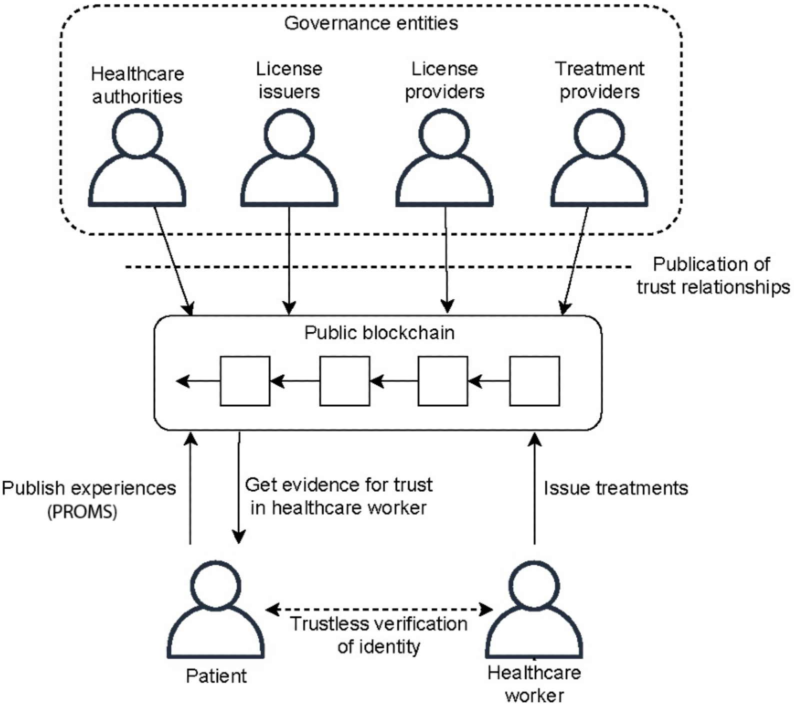


Overall Reference Architecture

Overview

As described in the functional requirements, the goal of VerifyMed is to provide trust in a health worker from a patient's perspective. The high-level reference architecture is shown in Figure 6. It captures trust by using a blockchain to store the formal trust relationship from health care organizations to health workers. Furthermore, as health workers issue treatments over time, summaries of these are published on blockchain. Finally, the evaluations of these treatments were published on the blockchain. The result is that the formal credentials of a practitioner can be validated through trust relationships, and their experience can be captured through logged treatments and evaluations.

Figure 6. The VerifyMed architecture for providing trust in a virtualized health care environment. PROMS: patient-reported outcome measures.



Creating Trust in a Caregiver

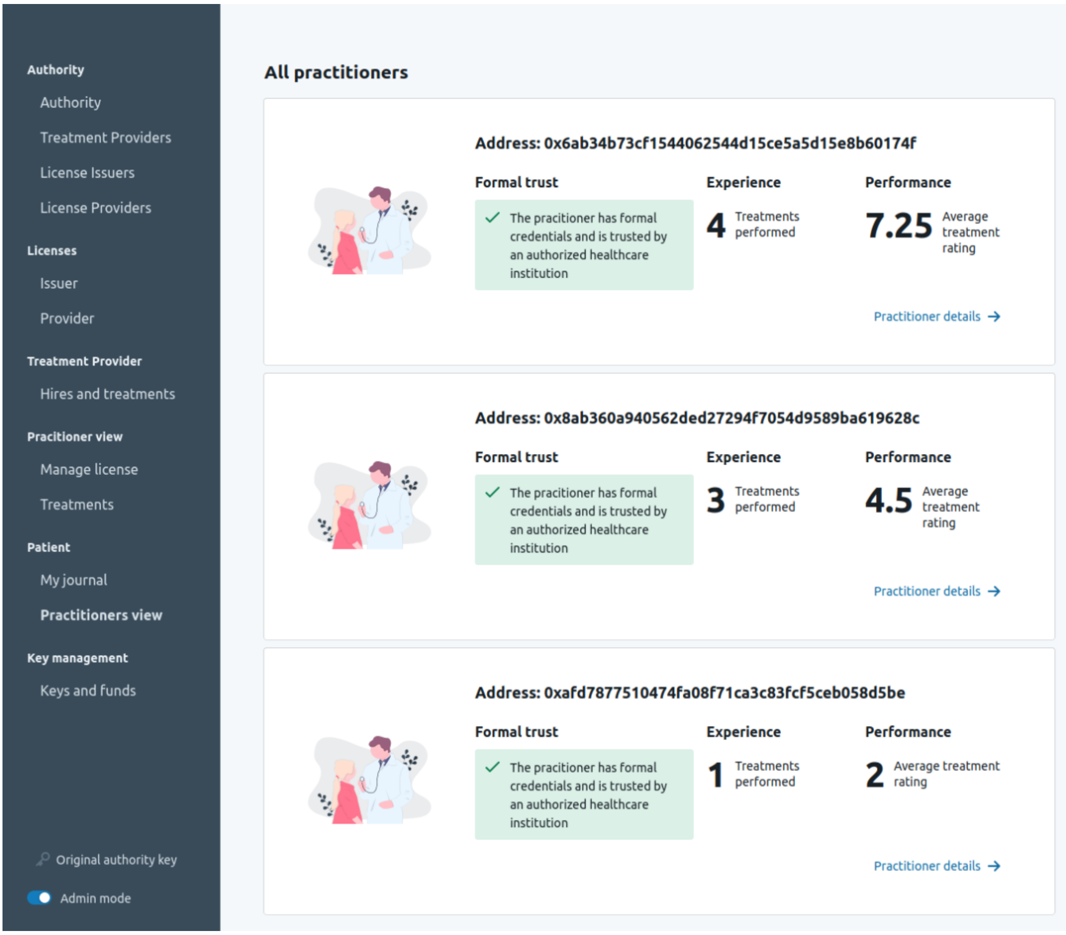
The first goal of the architecture is to capture the formal trust relationships between organizational actors and care providers within the health care industry. The end goal is to form a deduced trust relationship from health care authorities to the care provider and to capture the relationship in a way that is transparent and can be validated by the patients.

Figure 5 describes our model for trust relations between organizations and care providers. The top level was composed of large health care authorities. Authorities organize themselves through a model of distributed governance, for example, through simple voting, where existing trusted authorities can vote for the addition or removal of an authority. The main role of authorities is to provide trust in the defined stakeholders, who issue, authorize, and hire license holders. License holders can only practice and otherwise interact with the blockchain if all their upstream relations are linked to an authority. The patient entity is not part of this trust hierarchy; that is, patients are invited to publish PROMs on the blockchain by the care providers who have a trusted license after a completed treatment or interaction.

Caregiver and Patient Interaction

Once a license is considered trusted through the relationships captured on the blockchain, patients can use this information to check it. When meeting a practitioner, they can use the procedures defined in the smart contracts to check if their license is trusted and valid. Figure 7 illustrates the verification of the license, experiences, and skills of health practitioners.

Figure 7. Verification overview of health practitioners.



All practitioners

Address: 0x6ab34b73cf1544062544d15ce5a5d15e8b60174f

Formal trust: ✓ The pracitioner has formal credentials and is trusted by an authorized healthcare institution

Experience: 4 Treatments performed

Performance: 7.25 Average treatment rating

Address: 0x8ab360a940562ded27294f7054d9589ba619628c

Formal trust: ✓ The pracitioner has formal credentials and is trusted by an authorized healthcare institution

Experience: 3 Treatments performed

Performance: 4.5 Average treatment rating

Address: 0xafd7877510474fa08f71ca3c83fcf5ceb058d5be

Formal trust: ✓ The pracitioner has formal credentials and is trusted by an authorized healthcare institution

Experience: 1 Treatments performed

Performance: 2 Average treatment rating

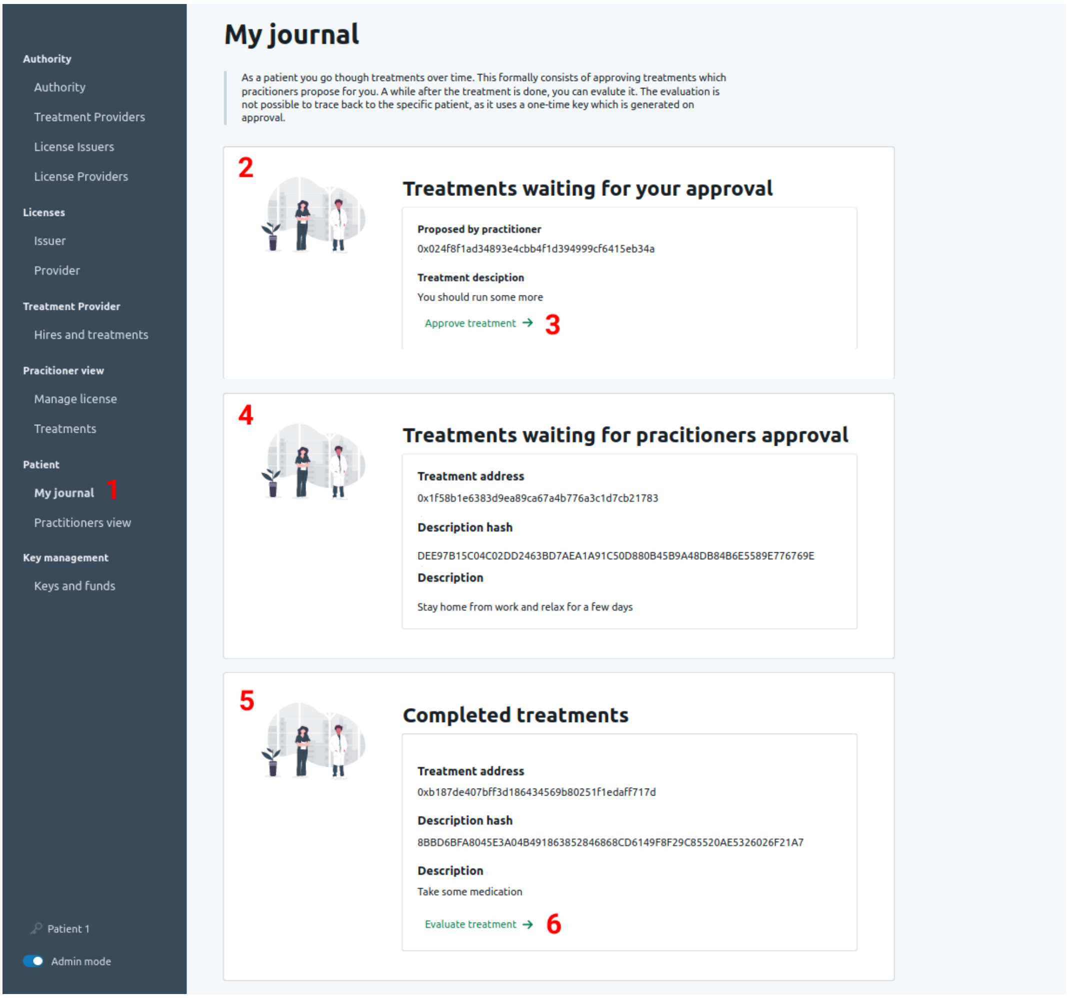
Evaluation of the Treatment

Once the treatment is completed, the patient may evaluate the treatment. The patient can do so via the one-time key generated during the treatment creation and thus create the evaluation without revealing their identity. This evaluation can be linked implicitly to a treatment provider and an approving practitioner. Future patients can use this information to enforce or decrease their trust in a practitioner.

Usage Outside of the Patient and Caregiver Relationship

Although we focus on the patient and caregiver relationship in the context of treatment, we also surface how public data sets have many use cases outside of this setting, such as audits, second opinion services, reporting, and evaluation of treatment providers. Figure 8 shows the user interface for the patients.

Figure 8. Overview of the user interface for patients.



My journal

As a patient you go though treatments over time. This formally consists of approving treatments which pracitioners propose for you. A while after the treatment is done, you can evalute it. The evaluation is not possible to trace back to the specific patient, as it uses a one-time key which is generated on approval.

Treatments waiting for your approval

Proposed by practitioner
0x024f8f1ad34893e4cbb4f1d394999cf6415eb34a

Treatment desciption
You should run some more

Approve treatment →

Treatments waiting for pracitioners approval

Treatment address
0x1f58b1e6383d9ea89ca67a4b776a3c1d7cb21783

Description hash
DEE97B15C04C02DD2463BD7AEA1A91C50D880B45B9A48DB84B6E5589E776769E

Description
Stay home from work and relax for a few days

Completed treatments

Treatment address
0xb187de407bff3d186434569b80251f1edaff717d

Description hash
8BBD6BFA8045E3A04B491863852846868CD6149F8F29C85520AE5326026F21A7

Description
Take some medication

Evaluate treatment →

Discussion

This work outlines a theoretical basis for the need for a blockchain enhanced trust model in a virtual health care setting, which contributes to the overall understanding of how the health care sector transforms into a new era, Healthcare 4.0, and the potential problems that could arise along with this transformation. Following this analysis, we built and implemented the novel VerifyMed platform that could trust in a virtualized health care environment.

We have used design principles from the Industry 4.0 concept to forecast Healthcare 4.0 and address an emerging problem in a future health care system. Our results show that our proof-of-concept implementation can be used to verify the authority of a health care worker, experience, and competence. The verifier does not have to place any trust in the health care workers themselves. This process can be performed by anyone with access to the Ethereum blockchain network, making the evaluation process fully transparent. In the further development of the system, microcredentialing can be incorporated, making it possible to verify specific skills among health care professionals.

Our trust model is justified in real-world governance of health care. As an environment with heavy regulatory oversight, capturing pre-existing governance relationships on a public blockchain serves as a natural first step for providing trust in virtualized settings. Furthermore, we strengthen our model by adding revocation abilities, where the trust of a governance entity can be revoked if it acts in bad faith. The result is a trust model justified in the inherited trust relationship between patients and the currently established health care system.

The VerifyMed platform enables individuals to store their respective credentials in a secure and accessible manner. The provenance of these data can be guaranteed using the immutability of the blockchain. In theory, this should mitigate the need to constantly verify the credentials from the issuing body and potentially speed up recruitment and onboarding processes in the health care sector.

We note that our trust model is extensible. A patient may trace all trust relationships from any evidence back to a top-level authority. The patient stands free to blindly trust the blockchain or use a third-party service to independently verify each of the upstream governance entities.

Health data are inherently sensitive, and thus, demand privacy. The management, storage, and access rights of health care data are highly regulated, both through general data protection acts such as the GDPR, health data specific acts such as the HIPAA, and often national health data laws. In an initial analysis [46], VerifyMed complies with the GDPR, although the general compliance of blockchain and the GDPR is under investigation; this work may have to be updated. Future work should include a comprehensive compliance analysis, and if appropriate, suggest an adaptation to comply with specific national health data laws and the HIPAA.

VerifyMed does not cover an identity solution for any of the users, and this is obviously an important component for the system to be ready for a real-life setting. As identity management is a core function in a health informatics system, future work must address this issue and develop an identity solution fitted to this particular use case.

VerifyMed uses the public Ethereum blockchain to host smart contracts. This choice is incorporated into the architecture, as the public nature of the blockchain is considered. Using a public blockchain requires limiting the published data to protect patient privacy, and access control schemes must be implemented within smart contracts. In addition, there is a need to incorporate a mechanism to transfer Ether (or smaller fractions of gas; ie, gwei or nanoeth) between accounts, thereby allowing them to submit transactions. The key advantage of using a public blockchain for this use case is transparency, no need for interorganizational agreements, and the possibility of interacting with the underlying cryptocurrency of Ethereum. The disadvantages of using the Ethereum blockchain are the monetary price of transactions and scalability issues related to low throughput. Furthermore, as the platform is governed by a set of authorities, license issuers, license providers, and treatment providers, this allows the publication of evidence for trust rooted in real-world trust relationships on the blockchain. This model contrasts with the fully trustless principles, which are usually applied within public blockchains but are necessary for the complex system of the health care domain. However, this can open up using a permissioned blockchain instead of fully public, which could have benefits such as reduced transaction costs and higher scalability. This should be explored in future studies.

VerifyMed could, with future updates, enrich the current trust model by including more trust requirements, such as (1) the caregiver must trust that the patient exists, (2) the caregiver must trust the authenticity of the data that the patient is willing to share, and (3) a third party (eg, an insurance company) must be able to trust the claim of the patient that care provision has taken place. The patient cannot really understand the credentials and experience of a caregiver because having a license is not the same as having credentials and having competency is not the same as having experience. Thus, the system should make the credentials or competency contextually important to the patient.

In the forecasting analysis, experts were consulted based on a convenience sample. This is not a comprehensive review of the general opinions of experts but just guidance in the direction of forecasting. It is not possible to preclude that this sample was not biased. However, a review of the literature supports input from expert consulting.

The trust mechanism that the blockchain enables in this concept provides a more transparent, accountable, and controlled handling of verifying competence and experience. This could also be achieved using a centralized solution. However, in the transition to Healthcare 4.0, decentralization is of increasing importance. This concept is consistent with this development.

Future research also needs to further validate the use case and the proof of concept of VerifyMed. Before modifying and updating the proof of concept, a feasibility study with real users should be undertaken to validate the concept and explore the interface design. The feasibility study could also address the challenge of how a patient interprets the presented verification of experience and verification of the competence of a caregiver.

Authors' Contributions

AH contributed to the conceptualization, methodology, visualization, writing, and original draft preparation. JAHR contributed to the data curation, software, and visualization. KK contributed to the writing, reviewing, supervision, and conceptualization. DG contributed to the writing, reviewing, supervision, visualization, and conceptualization. AF was involved with the conceptualization, methodology, visualization, writing, reviewing, and supervision.

Conflicts of Interest

None declared.

References

1. Oppers E, Chikada K, Eich F, Imam P, Kiff J, Kisser M, et al. The financial impact of longevity risk. In: Global Financial Stability Report: The Quest for Lasting Stability. Washington, DC: International monetary fund; Apr 1, 2012:37.
2. Harris RE. Epidemiology of Chronic Disease: Global Perspectives: Global Perspectives. Burlington, Massachusetts, USA: Jones & Bartlett learning; 2019.
3. Bongaarts J. Global fertility and population trends. Semin Reprod Med 2015 Jan;33(1):5-10. [doi: 10.1055/s-0034-1395272] [Medline: 25565505]

4. Raikwar M, Gligoroski D, Kralevska K. SoK of used cryptography in blockchain. IEEE Access 2019;7:148550-148575. [doi: 10.1109/access.2019.2946983]
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin Org. 2019. URL: https://bitcoin.org/bitcoin.pdf [accessed 2021-07-13]
6. Mohanta BK, Panda SS, Jena D. An Overview of Smart Contract and Use Cases in Blockchain Technology. In: 9th International Conference on Computing, Communication and Networking Technologies. 2018 Jul 10 Presented at: ICCCNT'18; July 10-12, 2018; Bengaluru, India p. 1-4. [doi: 10.1109/icccnt.2018.8494045]
7. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences-a scoping review. Int J Med Inform 2020 Feb;134:104040 [FREE Full text] [doi: 10.1016/j.ijmedinf.2019.104040] [Medline: 31865055]
8. Buterin V. Blockchain Lab. 2014. URL: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [accessed 2021-07-13]
9. Rolfe T. Turing Completeness and Smart Contract Security. Medium -Where Good Ideas Find You. 2019 Feb 1. URL: https://medium.com/kadena-io/turing-completeness-and-smart-contract-security-67e4c41704c [accessed 2021-05-08]
10. Kuo T, Rojas HZ, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. J Am Med Inform Assoc 2019 May 1;26(5):462-478 [FREE Full text] [doi: 10.1093/jamia/ocy185] [Medline: 30907419]
11. Zhang M, Walker MA, White J, Schmidt DC, Lenz G. Metrics for Assessing Blockchain-based Healthcare Decentralized Apps. In: 19th International Conference on e-Health Networking, Applications and Services. 2017 Dec 18 Presented at: IEEE'17; October 12-15, 2017; Dalian, China. [doi: 10.1109/healthcom.2017.8210842]
12. Schmidt P. Blockcerts - An Open Infrastructure for Academic Credentials on the Blockchain. Medium - Where Good Ideas Find You. 2016 Oct 24. URL: https://tinyurl.com/6f3jeb5t [accessed 2021-07-13]
13. Baldi M, Chiaraluce F, Kodra K, Spalazzi L. Security Analysis of a Blockchain-based Protocol for the Certification of Academic Credentials. arXiv.org e-Print archive. 2019. URL: https://arxiv.org/abs/1910.04622 [accessed 2021-07-13]
14. A Digital Exchange for Professional Credentials Data. Hashed Health. 2020. URL: https://hashedhealth.com/blockchain-healthcare-solutions/professional-credentials-exchange/ [accessed 2021-05-01]
15. Axuall, Inc. and MetroHealth Announce Collaboration to Improve and Streamline Practitioner Credentialing. PR Newswire. 2020. URL: https://www.prnewswire.com/news-releases/axuall-inc-and-metrohealth-announce-collaboration-to-improve-and-streamline-practitioner-credentialing-300997828.html [accessed 2021-05-01]
16. Campbell M, Fitzpatrick R, Haines A, Kinmonth AL, Sandercock P, Spiegelhalter D, et al. Framework for design and evaluation of complex interventions to improve health. Br Med J 2000 Sep 16;321(7262):694-696 [FREE Full text] [doi: 10.1136/bmj.321.7262.694] [Medline: 10987780]
17. Doos L, Packer C, Ward D, Simpson S, Stevens A. Past speculations of the future: a review of the methods used for forecasting emerging health technologies. BMJ Open 2016 Mar 10;6(3):e010479 [FREE Full text] [doi: 10.1136/bmjopen-2015-010479] [Medline: 26966060]
18. Pohl K. Requirements Engineering Fundamentals, Principles, and Techniques. Berlin/Heidelberg, Germany: Springer Publishing Company; Jul 23, 2010.
19. Hevner, March, Park, Ram. Design science in information systems research. MIS Quarterly 2004;28(1):75. [doi: 10.2307/25148625]
20. Thuemmler C. In: Thuemmler C, Bai C, editors. Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare. Swizerland: Springer International Publishing; 2017.
21. Lasi H, Fettke P, Kemper H, Feld T, Hoffmann M. Industry 4.0. Bus Inf Syst Eng 2014 Jun 19;6(4):239-242. [doi: 10.1007/s12599-014-0334-4]
22. Hermann M, Pentek T, Otto B. Design principles for Industrie 4.0 scenarios. In: 49th Hawaii International Conference on System Sciences. 2016 Mar 10 Presented at: HICSS'16; January 5-8, 2016; Koloa, HI, USA. [doi: 10.1109/hicss.2016.488]
23. Gregor S. A Theory of Theories in Information Systems. Information Systems Foundations: Building the Theoretical Base. 2002. URL: https://tinyurl.com/ua9ka254 [accessed 2021-07-13]
24. McKnight D, Chervany N. Trust and distrust definitions: one bite at a time. In: Trust in Cyber-societies Integrating the Human and Artificial Perspectives. Berlin, Heidelberg, Germany: Springer; Dec 20, 2001:27-54.
25. Rousseau DM, Sitkin SB, Burt RS, Camerer C. Not so different after all: a cross-discipline view of trust. Acad Manag Rev 1998 Jul 1;23(3):393-404. [doi: 10.5465/Amr.1998.926617]
26. Coulter A. Patients' views of the good doctor. Br Med J 2002 Sep 28;325(7366):668-669 [FREE Full text] [doi: 10.1136/bmj.325.7366.668] [Medline: 12351342]
27. Mechanic D, Schlesinger M. The impact of managed care on patients' trust in medical care and their physicians. J Am Med Assoc 1996 Jun 5;275(21):1693-1697. [Medline: 8637148]
28. The duties of a doctor registered with the General Medical Council. General Medical Council. 1998. URL: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/good-medical-practice/duties-of-a-doctor [accessed 2021-07-13]
29. The Nurse's Code: A Practical Approach to the Code of Professional Conduct for Nurses, Midwives and Health Visitors. London, UK: The British Psychological Society; 2018.

Croker JE, Swancutt DR, Roberts MJ, Abel GA, Roland M, Campbell JL. Factors affecting patients' trust and confidence in GPs: evidence from the English national GP patient survey. BMJ Open 2013 May 28;3(5):- [FREE Full text] [doi: 10.1136/bmjopen-2013-002762] [Medline: 23793686]

Sakallaris BR, Miller WL, Saper R, Kreitzer MJ, Jonas W. Meeting the challenge of a more person-centered future for US healthcare. Glob Adv Health Med 2016 Jan;5(1):51-60 [FREE Full text] [doi: 10.7453/gahmj.2015.085] [Medline: 26937314]

Leimeister JM, Ebner W, Krcmar H. Design, implementation, and evaluation of trust-supporting components in virtual communities for patients. J Manag Inf Syst 2014 Dec 8;21(4):101-131. [doi: 10.1080/07421222.2005.11045825]

O´neill O. Intelligent trust in a digital world. New Perspect Q 2017 Oct;34(4):27-31. [doi: 10.1111/npqu.12105]

Hall MA, Zheng B, Dugan E, Camacho F, Kidd KE, Mishra A, et al. Measuring patients' trust in their primary care providers. Med Care Res Rev 2002 Sep;59(3):293-318. [doi: 10.1177/1077558702059003004] [Medline: 12205830]

Pearson SD, Raeke LH. Patients' trust in physicians: many theories, few measures, and little data. J Gen Intern Med 2000 Jul;15(7):509-513 [FREE Full text] [doi: 10.1046/j.1525-1497.2000.11002.x] [Medline: 10940139]

Frow P, McColl-Kennedy JR, Payne A. Co-creation practices: Their role in shaping a health care ecosystem. Ind Mark Manag 2016 Jul;56:24-39. [doi: 10.1016/j.indmarman.2016.03.007]

Montague EN, Kleiner BM, Winchester WW. Empirically understanding trust in medical technology. Int J Ind Ergon 2009 Jul;39(4):628-634. [doi: 10.1016/j.ergon.2009.01.004]

Technical Report. CompData. 2017. URL: https://tinyurl.com/ek2s8pwa [accessed 2021-07-13]

Najib M, Abdullah S, Narresh S, Juni MH. Brain-drain phenomenon among healthcare workers. Int J Public Health Clin Sci 2019 Jun 1;6(3):90-103. [doi: 10.32827/ijphcs.6.3.90]

Sabesan S, Kelly J, Evans R, Larkins S. A tele-oncology model replacing face-to-face specialist cancer care: perspectives of patients in North Queensland. J Telemed Telecare 2014 Jun;20(4):207-211. [doi: 10.1177/1357633X14529237] [Medline: 24643950]

Andreassen HK, Trondsen M, Kummervold PE, Gammon D, Hjortdahl P. Patients who use e-mediated communication with their doctor: new constructions of trust in the patient-doctor relationship. Qual Health Res 2006 Feb;16(2):238-248. [doi: 10.1177/1049732305284667] [Medline: 16394212]

Rensaa H. Verifymed - Application of Blockchain Technology to Improve Trust in Virtualized Healthcare Services. ResearchGate. Trondheim: Norwegian University of Science and Technology (NTNU); 2020 Jun 1. URL: https://www.researchgate.net/publication/349251550_VerifyMed_-_Application_of_blockchain_technology_to_improve_trust_in_virtualized_healthcare_services [accessed 2021-07-13]

Rensaa H, Gligoroski D, Kralevska K, Hasselgren A, Faxvaag A. Verifymed-a Blockchain Platform for Transparent Trust in Virtualized Healthcare: Proof-of-concept. In: Proceedings of the 2020 2nd International Electronics Communication Conference. 2020 Jul Presented at: IECC'20; July 8-10, 2020; Singapore p. 73-80. [doi: 10.1145/3409934.3409946]

Rensaa J. Transparent healthcare. GitHub. 2020. URL: https://github.com/jarensaa/transparent-healthcare [accessed 2021-05-01]

van Eecke P, Haie A. Practitioner’s corner · blockchain and the GDPR: the EU blockchain observatory report. Eur Data Prot L Rev 2018;4(4):531-534. [doi: 10.21552/edpl/2018/4/18]

Hasselgren A, Wan P, Horn M, Kralevska K, Gligoroski D, Faxvaag A. GDPR Compliance for Blockchain Applications in Healthcare. In: International Conference on Big Data, IoT and Blockchain. 2020 Oct Presented at: BIBC'20; October 24-25, 2020; Dubai, UAE URL: https://app.cristin.no/projects/show.jsf?id=2041854 [doi: 10.5121/csit.2020.101303]

bbreviations

dApps: decentralized applications
GDPR: General Data Protection Regulation
HIPAA: American Health Insurance Portability and Accountability Act
PROM: patient-reported outcome measure

Edited by R Kukafka; submitted 04.03.21; peer-reviewed by R El-Gazzzar, D Cabrera, T Ueno, C Reis, TT Kuo; comments to author 26.04.21; revised version received 19.05.21; accepted 14.06.21; published 30.07.21

Please cite as:
Hasselgren A, Hanssen Rensaa JA, Kralevska K, Gligoroski D, Faxvaag A
Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study
J Med Internet Res 2021;23(7):e28496
URL: https://www.jmir.org/2021/7/e28496
doi: 10.2196/28496
PMID: 34328437

C

Hasselgren, A., Kralevska, K., Gligoroski, D. and Faxvaag, A., 2021. Medical Students' Perceptions of a Blockchain-Based Decentralized Work History and Credentials Portfolio: Qualitative Feasibility Study. JMIR Formative Research, 5(10), p.e33113.

Original Paper

Medical Students’ Perceptions of a Blockchain-Based Decentralized Work History and Credentials Portfolio: Qualitative Feasibility Study

Anton Hasselgren[1], MSc; Katina Kralevska[2], PhD; Danilo Gligoroski[2], PhD; Arild Faxvaag[1], MD, PhD

[1]Department of Neuromedicine and Movement Science, Norwegian University of Science and Technology, Trondheim, Norway

[2]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim, Norway

Corresponding Author:
Anton Hasselgren, MSc
Department of Neuromedicine and Movement Science
Norwegian University of Science and Technology
Mellomila 71
Trondheim, 7018
Norway
Phone: 47 46948498
Email: anton.hasselgren@ntnu.no

Abstract

Background: Increased digitization of health care might challenge some of the trust functions that are established in a traditional health care system. We have, with the concept of VerifyMed, developed a decentralized service for work history and competence verification, as a means to increase trust in the virtual interaction between a patient and a caregiver, mitigate administrative burden, and provide patient-reported outcomes seamlessly for health professionals.

Objective: This research aimed to validate the use case of a decentralized credentials service for health care professionals in Norway. We also aimed to evaluate the proof-of-concept of VerifyMed, a blockchain-based credential service for health care professionals.

Methods: A qualitative approach was applied with data collection through 9 semistructured interviews and 2 focus groups (one with 4 participants and the other with 5 participants). The System Usability Scale (SUS) was used as a part of the interviews. Data were analyzed through the principles of systematic text condensation. The recruitment of participants ended when it was concluded that the data had reached saturation.

Results: The following 5 themes were identified from the interviews and focus groups: (1) the need for aggregated storage of work- and study-related verification, (2) trust in a virtual health care environment, (3) the potential use of patient feedback, (4) trust in blockchain technology, and (5) improvements of the VerifyMed concept. The SUS questionnaire gave a score of 69.7.

Conclusions: This study has validated the need for a decentralized system where health care professionals can control their credentials and, potentially, their reputation. Future work should update the VerifyMed system according to this input. We concluded that a decentralized system for the storage of work-related verifiable credentials could increase trust in a virtualized health care system.

(JMIR Form Res 2021;5(10):e33113) doi: 10.2196/33113

KEYWORDS

blockchain; eHealth; qualitative research; VerifyMed

Introduction

Background

The COVID-19 pandemic has accelerated the digital transformation of the health care sector. Social distancing and other measures to reduce transmission of SARS-CoV-2 have forced health systems to deliver health services using innovative methods [1]. Virtual health care consultations, which often are referred to as telemedicine, are an example of this transformation that has had a rapid increase during the pandemic. Telemedicine visits increased by 683% in New York City during the spring of 2020 [2], and general practitioners in Norway reported that

81% of them used video consultation during the pandemic (most of them did not use it at all before the pandemic) [3]. Since the advantages of telemedicine include cost-effectiveness, increased access, and availability [4], we can assume that this increase will be permanent. In previous work, it was suggested that telemedicine might challenge some of the established structures for trust in a patient–health care professional relationship [5]. The ability to verify the competence of health care professionals will be of increasing importance in telemedicine in order to enhance trust [6,7].

The administrative burden placed on health care professionals has perhaps always been present [8]. However, the administrative burden related to work mobility seems to have increased recently [9], and this trend is also reflected in increased mobility among health care professionals [10]. As a result, the administrative burden of verifying credentials and experiences among this working group is increasing.

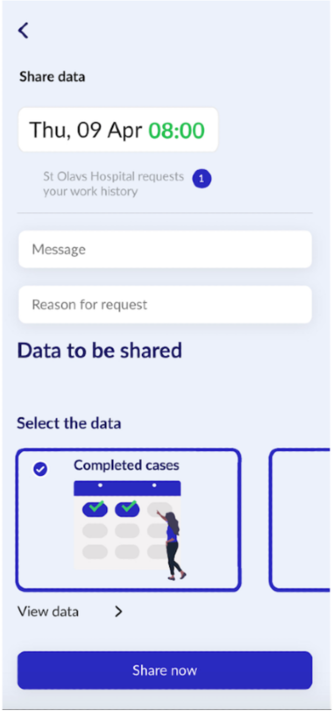
For the last decades, there has been a focus on putting patients in the center of evaluating clinical care, combined with biomarkers of health improvements [11]. As a mean for this, patient-reported outcome measures (PROMs) have been introduced to measure patient-reported outcomes (PROs). PROs are referred to as the patient's health, quality of life, or functional status associated with health care or treatment [12]. PROMs are the tools to measure PROs, which could, for example, be a measure of the quality of life. To complement PROMs, patient-reported experience measures (PREMs) have been introduced as a tool to measure patients' experiences with health care or health services, often with a satisfactory score [12]. PROs may have increasing importance as a means of learning and improving health care professionals, as well as a way for health care professionals to verify their work history [13].

We have identified a need for a new decentralized service for work history and competence verification as a means to increase trust in the virtual interaction between a patient and a caregiver, mitigate administrative burden, and provide PROs seamlessly for health professionals. This concept is described in the next subsection.

VerifyMed

The proposed concept of VerifyMed provides a solution for enhancing trust between a caregiver and a patient within a virtualized health care environment. The cornerstone of this architecture is an approach for capturing the trust relationships within the health care system by utilizing a blockchain. This trust mechanism can be used by patients to confirm the credentials and potentially enhance their trust in a caregiver during their interaction. Furthermore, the architecture includes a mechanism for evaluating these interactions publicly on the blockchain, using PROMs and PREMs. These evaluations serve as a portfolio of the caregiver's experience and could potentially be used as a mechanism for continued learning among health care professionals. The concept of VerifyMed is presented further in other reports [5,14,15]. To achieve the objectives of this research, a mock-up of the user interface of the platform was designed using user-centric design theory [16]. The mock-up can be accessed online [17]. Figure 1 and Figure 2 illustrate examples of the user interface that was explored in this research.

Figure 1. The data sharing page of the VerifyMed user interface.



Share data

Thu, 09 Apr 08:00

St Olavs Hospital requests your work history 1

Message

Reason for request

Data to be shared

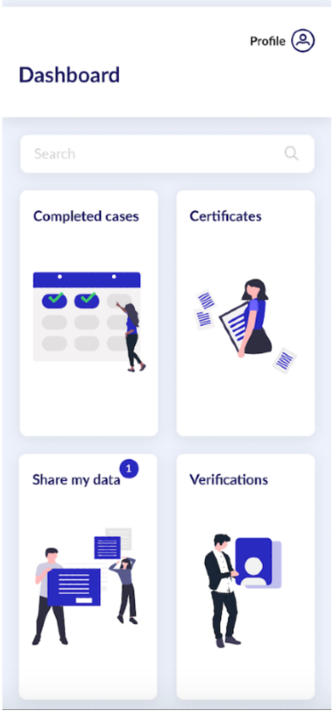
Select the data

Completed cases

View data >

Share now

Figure 2. The dashboard page of the VerifyMed user interface.



Profile

Dashboard

Search

Completed cases

Certificates

Share my data 1

Verifications

Significance

It is important to gain user input early in technology development to further improve an application according to the needs of the users [18]. After identifying a problem in the health sector and designing a solution for that problem with a proof-of-concept, a feasibility study further validates the concept of VerifyMed and provides valuable user input for further development.

Aim and Objective

The objective of this work was 2-fold. First, the work aimed to validate a use case of a decentralized medical professional credentials service by mapping out the need for such a service in Norway. Second, we aimed to evaluate the proof-of-concept of VerifyMed, a blockchain-based credential service for health care professionals. We limited the scope of the work to medical students, as they might experience challenges with recording and managing their credentials and experience as they start and progress through their careers.

Research Questions

The research questions were as follows:

1. What are the potential scenarios of usage from the user group?
2. How will a decentralized system, such as VerifyMed, be accepted by future health care professionals?
3. Does the VerifyMed system meet the requirements of health care professionals who would be using the system?
4. What are the desired features of the users?
5. What are the opinions on a patient-feedback system?

Methods

Overview

To answer the research questions, a qualitative approach was applied. Data were collected through 9 semistructured interviews by using the System Usability Scale (SUS) [19] as a starting point for the interviews. In addition, 2 focus groups (one with 4 participants, and the other with 5 participants) were also conducted. The recruitment of participants ended when it was concluded that the data had reached saturation [20].

Data Collection

Medical students in Norway in study years 4 to 6 were recruited through student organizations. Two focus groups were performed prior to the individual interviews. The focus groups functioned as workshops where blockchain technology [21] and the concept of VerifyMed were presented by the moderator (AH) before any discussion. The moderator asked the participants to describe the current procedures they had experienced with skill verification, certificates, and trust in a virtual health care scenario. Finally, an open discussion on how the presented technology could be used to improve the current workflows was initiated. The focus groups were limited to 45 min. In addition to the moderator, a research assistant was present to take notes.

The duration of the individual interviews was limited to 30 min. The participants were invited to the mock-up of the VerifyMed user interface by an online link. They accessed the mock-up through their web browsers on their laptops. After a short introduction, each participant was invited to perform several simple tasks in the prototype and was asked to explain his or her thoughts during this exploration phase, with minimal assistance from the moderator. The participant was then asked questions from the SUS questionnaire. The SUS is considered to be an easy, quick, and reliable test of usability that is technology agnostic [19]. Based on the answers, follow-up questions followed in a semistructured form. The focus groups and the individual interviews were conducted in an online format, using Zoom (Zoom Video Communications).

Data Management

The focus group sessions and the user-testing interviews were audio and video recorded. The recordings were analyzed after the sessions by the main researcher (AH). The 3 other researchers in the project (AF, KK, and DG) also reviewed the recordings when there were doubts by the first researcher. The recordings were stored locally on the first researcher's computer during the project. The recordings were transcribed and erased after transcription, and the notes from the focus group sessions were compared with the transcripts and then erased.

Data Analysis

Transcription of the collected data was performed according to the 6 steps of transcription proposed by Azevedo et al [22]. Since the data collection was conducted in Norwegian, an English translation of the used quotations was performed by the main researcher (AH). Data were analyzed according to the principles of systematic text condensation [23]. This procedure consists of the following 4 steps: (1) getting a total impression by reading all the text materials and identifying preliminary themes; (2) identifying meaningful units from both the technical aspects of the VerifyMed service and its use by medical students; (3) abstracting condensates from each group and subgroup; and (4) creating synthesized descriptions of the user's experiences and opinions about the use of a decentralized work history portfolio. The software NVivo (version 1.4.1; QSR International) was used for the analysis.

Ethical Considerations

All participants were asked to give written consent based on oral and written information about the study. Only those who gave their consent to participate in the study, according to the information in the consent form, were included (n=9). The study did not collect or otherwise handle patient- or health-related data. Therefore, ethical clearance from the Regional Ethical Committee (REK) was not obtained. The study was registered by NSD - Norwegian Center for Research Data and the Data Protection Officer at the Faculty of Medicine and Health Science (Norwegian University of Science and Technology) to be General Data Protection Regulation compliant.

Results

Participant Characteristics

A total of 9 participants were recruited in the study, and all 9 completed both participation in the focus group and the individual interview. The characteristics of the respondents are presented in Table 1.

Table 1. Characteristics of the informants.

Characteristic	Value (n=9), n (%)
Gender	
Male	4 (44)
Female	5 (56)
Age (years)	
23-24	3 (33)
25-26	2 (22)
27-28	3 (33)
>28	1 (11)
Study year (out of 6)	
4	1 (11)
5	5 (56)
6	3 (33)
University	
Norwegian University of Science and Technology	8 (89)
University of Oslo	1 (11)
Previous knowledge of blockchain	
No	6 (67)
Yes	3 (33)

Themes

The results from the SUS were mainly used as a starting point for the individual interviews. The quantitative results from the SUS were calculated using the standard formula for SUS [24]. The score was 69.7, with fairly equal responses from the respondents. A score above 70 is considered acceptable, according to validation studies [24]. In the data analysis, 5 themes were identified within the focus groups and individual interviews, and an overview is presented in Table 2. The results from both methods of data collection were intertwined. Several of the themes were discussed in both the focus groups and individual interviews, and they are therefore presented here jointly.

Table 2. Results overview.

Theme	Proportion[a] of data	Supporting quotes
The need for an aggregated storage of work- and study- related verifications	24.2%	*...large parts of the system is trust based. I don't know how to verify certificates, but as you say, paper-based certificates are an easy way to falsify knowledge and experience.*
Trust in a virtual health care environment	26.0%	*To showcase what you have done related to courses and such could contribute, it becomes the equivalent to have diplomas on the wall. It is not necessarily certain that the patient understands what it is, but it can improve the total impression.*
The potential use of patient feedback	14.5%	*The ones who write feedback are the patients how are either very pleased or they who are very displeased. ...the selection gets skewed.*
Trust in blockchain technology	7.3%	*I think I understand the value with that things could be verified and that falsification might be mitigated with time-stamping and such, that I see as positive...*
Improvements of the VerifyMed concept	6.5%	*I envision that in the future, when things get more digital and patients have a specific problem and want to get in contact with a doctor who has done research in that area or has any specific courses within the area...*

[a] The percentages do not add to 100 since other themes, not relevant to the research questions, also were discussed.

The Need for an Aggregated Storage of Work- and Study-Related Verifications

The first theme evolves around the need for a platform where medical students can collect and store verifications of their experiences. As the participants describe, as of now, there is no common digital system in use where they can store grades, certificates, references, and verifications of practical assignments. One participant expressed this as follows:

> *...it would be nice if it could be done digitally. Previously in the studies, we rotated to different departments of the hospital and were supposed to get one signature from each department. We were supposed to keep this piece of paper with over 20 signatures throughout the semester and try to not lose it. It would be an advantage if this could be done digitally.*

If this physical paper is lost by the students, they need to collect all the signatures again. This was expressed as a rather common problem and a lot of work. On this occasion, it seems like the supervisors were not always aware of what they approved by giving their signatures.

> *...if you needed to go back for the signature, it could happen that they were a bit uncertain but most of the time they signed anyway, or always.*

The risk of falsified documents with an analog trust-based system was further acknowledged in the discussion. As one respondent expressed:

> *...large parts of the system is trust-based. I don't know how to verify certificates, but as you say, paper-based certificates are an easy way to falsify knowledge and experience.*

Trust in a Virtual Health Care Environment

The second identified theme evolves around trust in the interaction between the medical doctor (student) and the patient. Since the respondents were in different stages of their education, they had experienced different exposures to patients. Their perceptions of trust in their encounters with patients also varied. Some respondents did experience a lack of trust towards them among patients.They expressed that this probably was a consequence of they being students and thus being considered less experienced and knowledgeable. However, most of the respondents experienced that trust could be established, and it was not considered a major disadvantage that they were students. Furthermore, trust in a virtual health care environment, mainly video consultations, was discussed. The respondents agreed that this way of providing health services will be an important part of their professional careers. They had so far been exposed to this medium in various degrees, mainly due to COVID-19, where restrictions enforced virtual meetings instead of physical meetings. Their perceptions of quality in virtual health services, compared to physical services, varied. Some experienced no difficulties in gaining the trust and confidence of patients. However, most seemed to agree that the lack of physical attributes and the lack of physical examinations may harm the trust-building mechanisms.

> *You get something for free in a hospital setting, you walk-in in a white coat, that looks professional. I believe most doctors perform virtual consultation from a setting that looks professional, otherwise, it can look suspicious.*

The individual interviews further explored the need for digital verifications, and the general opinions among the respondents were that this could have a purpose in a virtual environment.

> *To showcase what you have done related to courses and such could contribute, it becomes the equivalent to have diplomas on the wall. It is not necessarily certain that the patient understands what it is, but it can improve the total impression.*

However, participants were also hesitant about how this information would be interpreted by the patients, and if they would comprehend the meaning of such certificates and other proofs of competence.

> *...I'm a bit uncertain regarding this. What value would it bring if they could see this, it might be difficult for them to interpret. It's difficult to say what they would use this information for.*

The Potential Use of Patient Feedback

The third theme identified was the expectations and fears around a patient-feedback system, such as PROs. In this discussion, the Norwegian website Legelisten [25], a site where anyone can rate their general practitioner, was referred to several times. The respondents' general opinions around this service were negative, and the patient-feedback system was associated with the negative impressions of this service. For example, the risk of a biased selection of users of this service was expressed as follows:

> *The ones who write feedback are the patients who are either very pleased or they who are very displeased. ...the selection gets skewed.*

The participants also expressed a general fear of being publicly rated, similar to the rating system of Legelisten [25]:

> *...agree that it could be an individual asset but nothing that should be published publicly, how good you are in comparison with others because that will create competition rather than provide you with learning.*

This fear also extended to how data could be reported in a feedback system. Several respondents expressed the need for this kind of feature to be objective and systematic. Allowing patients to provide feedback without any systematic framework was expressed as being associated with a major risk of information overload and useless information from the patients.

> *...maybe you should not be able to write free text with no limit and maybe you should limit how the feedback is given, otherwise it will be a lot of irrelevant and unserious feedback, so it has to be a limitation for the patients' possibility to provide feedback.*

A feedback system as a means for health care professionals to learn was however expressed as something positive among the participants. At present, they have little or no opportunity to know the outcome of a given patient treatment, since they often rotate and may miss a revisit or the results when the patient gets referred to another department.

> *You often wonder how it went and what happened to the patient.*
>
> *It would be great to get a small correction and feedback on what you have done and how it went, and what conclusions were made further. That would be gold worth to know...*

Trust in Blockchain Technology

The fourth theme, trust in blockchain technology, was briefly discussed. As Table 1 indicates, a few of the respondents had knowledge about blockchain technology prior to participating in this research. Even though blockchain was introduced in a presentation by the moderator (AH) before the focus group discussions, several of the respondents reported that they did not understand the technology. However, none of them showed any negativity toward the technology and whether to trust the VerifyMed service.

> *I think I understand the value with that things could be verified and that falsification might be mitigated with time-stamping and such, that I see as positive. But I don't know enough about the technology to say if it gives any large advantages compared to other services. I think I understand it, but I'm not a technical person.*

As expressed by several respondents, the trust in the service was dependent on third-party validation and trust in the developers behind the service. One respondent commented as follows:

> *Yes, if the source is trustworthy and it helps if it is promoted by persons you trust. ...but if it is an unknown actor which I could not relate to I would be much more skeptical to provide any personal information.*

Improvements of the VerifyMed Concept

The last main theme that was discussed were general improvements and opinions regarding the VerifyMed user design and features experienced by all respondents. None of the respondents had any problems completing the 9-item task list given, and they all did so in a short amount of time (3-7 min). The general expression was that the solution could be useful and that they acknowledge the need for this kind of service. One respondent commented as follows:

> *I envision that in the future, when things get more digital and patients have a specific problem and want to get in contact with a doctor who has done research in that area or has any specific courses within the area, then it could be very useful for both the doctor to be able to show knowledge and interests in that particular area, then you might get more patients you can include in your research or that you find interesting.*

The informants expressed that the design and user flow were something that they were familiar and comfortable with. They had a few suggestions on improvements and additions of features, such as (1) make it clearer what data are being shared, for how long, and with whom, (2) make it possible to have direct communication with patients through a message system, and (3) make it possible to showcase scientific publications or research projects as a part of the "portfolio."

Discussion

Principal Findings

This research aimed to validate a use case of a decentralized medical professional credentials service by mapping out the need for such a service in Norway and to evaluate the proof-of-concept of VerifyMed, a blockchain-based credentials service for health care professionals.

The informants expressed that the main area of use is a platform where they could store all the data they would need for a job application. This is perhaps an expected result since the respondents are already (or will soon be) in a job-seeking process. The general opinion was that they had no or little control over data, such as verifications of internships or practical assignments, at present. They were all positive about the idea of a system that could automate this and provide them with more control. Presently, it seems to be somewhat up to chance if they receive these paper-based verifications and how useful they are owing to a lack of systematization. This highlights the need for new services with features similar to those of VerifyMed.

Fear was generally expressed for a patient-feedback system among the participants, in case the data are used to evaluate them externally. This fear might be explained by the fact that young physicians (students) are already exposed to a lot of stress and have a fear of making mistakes [26]. The addition of another evaluation service could increase this stress. However, they were generally positive about receiving feedback for their own learning. They were also open to extend this and share the feedback with colleagues and take part in each other's feedback, for the objective of learning. Previous research has indicated that it might be difficult for health care professionals to learn from patient feedback [27]. The sample in this study (students) might explain this difference, as students are probably more inclined to learn and improve compared to more senior health care professionals. They did however see little or no use in sharing patient feedback with other patients, as they did not see the need for this. This is in line with previous research [28]. The existence of physician-rating websites, such as Legelisten [25], indicates that patients are interested in the feedback of other patients to evaluate physicians. This difference in perception between physicians and patients might again be explained by physicians' fears of being evaluated and potentially not having control over their reputation as health care professionals. Previous research has indicated that a physician's reputation on physician-rating websites is critical to attract patients [29], and there seems to be a lack of tools where physicians can take control over their online reputation [30]. This previous knowledge and our results clearly indicate the need for a service where physicians can control their online reputation. Considering this, future updates on the VerifyMed concept should include options to share or not to share patient feedback publicly. This control feature might enhance the acceptability of the service among health care professionals and enable reputation control in a virtualized health care environment.

The quantitative results from the SUS should be interpreted with the understanding that the small sample size prevents any strong conclusions from this quantitative result. However, it could serve as an indicator that the usability of the user design is acceptable [24] (the study showed a SUS score of 70). There were no indications that design changes need to be implemented in the platform based on the user testing.

The limited clinical experience of the informants may have influenced the results, and it is possible that another sample, with more experienced health care professionals, will have other opinions. However, the results from the current informant sample fulfill the objectives of this research. The individual interviews might have been influenced by the discussions in the focus groups and the presentation made by the main researcher (AH), which were both conducted before the individual interviews. The perception of the technology might have been influenced as a result.

Conclusion

This study validated the need for the concept of VerifyMed, and feedback from the users provided inputs that will further enhance the quality and fit-for-purpose aspect of the concept. Future work should update the system according to these inputs, enhance the data control of the user to provide reputation control, and move to the next step of system development. Furthermore, we concluded that a decentralized system for the storage of work-related verifiable credentials could increase trust in the health system, especially if there are less trusted institutions as a result of an increase in the number of health care providers in a digitally transformed health care system.

Acknowledgments

The authors acknowledge the contributions of Cathrin Brønbo Larsen, who assisted with validating the interview and focus group formats and took notes during the focus group sessions. Martha Skogen assisted with the validation of the mock-up design, and Torunn Hatlen Nøst assisted with the validation of the focus group format.

Conflicts of Interest

None declared.

References

1. Webster P. Virtual health care in the era of COVID-19. The Lancet 2020 Apr;395(10231):1180-1181. [doi: 10.1016/s0140-6736(20)30818-7]
2. Mann DM, Chen J, Chunara R, Testa PA, Nov O. COVID-19 transforms health care through telemedicine: Evidence from the field. J Am Med Inform Assoc 2020 Jul 01;27(7):1132-1135 [FREE Full text] [doi: 10.1093/jamia/ocaa072] [Medline: 32324855]
3. Johnsen TM, Norberg BL, Kristiansen E, Zanaboni P, Austad B, Krogh FH, et al. Suitability of Video Consultations During the COVID-19 Pandemic Lockdown: Cross-sectional Survey Among Norwegian General Practitioners. J Med Internet Res 2021 Feb 08;23(2):e26433 [FREE Full text] [doi: 10.2196/26433] [Medline: 33465037]
4. Kichloo A, Albosta M, Dettloff K, Wani F, El-Amir Z, Singh J, et al. Telemedicine, the current COVID-19 pandemic and the future: a narrative review and perspectives moving forward in the USA. Fam Med Community Health 2020 Aug 18;8(3):e000530 [FREE Full text] [doi: 10.1136/fmch-2020-000530] [Medline: 32816942]
5. Hasselgren A, Hanssen Rensaa J, Kralevska K, Gligoroski D, Faxvaag A. Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study. J Med Internet Res 2021 Jul 30;23(7):e28496 [FREE Full text] [doi: 10.2196/28496] [Medline: 34328437]
6. Pearson SD, Raeke LH. Patients' trust in physicians: many theories, few measures, and little data. J Gen Intern Med 2000 Jul;15(7):509-513 [FREE Full text] [doi: 10.1046/j.1525-1497.2000.11002.x] [Medline: 10940139]
7. O'Neill O. Intelligent Trust in a Digital World. New Perspectives Quarterly 2007 Nov 06;34(4):27-31. [doi: 10.1111/npqu.12105]
8. Woolhandler S, Himmelstein DU. Administrative Work Consumes One-Sixth of U.S. Physicians' Working Hours and Lowers their Career Satisfaction. Int J Health Serv 2014 Oct 01;44(4):635-642. [doi: 10.2190/hs.44.4.a]
9. Rao SK, Kimball AB, Lehrhoff SR, Hidrue MK, Colton DG, Ferris TG, et al. The Impact of Administrative Burden on Academic Physicians. Academic Medicine 2017;92(2):237-243. [doi: 10.1097/acm.0000000000001461]
10. Costigliola V. Mobility of medical doctors in cross-border healthcare. EPMA J 2011 Dec 12;2(4):333-339 [FREE Full text] [doi: 10.1007/s13167-011-0133-7] [Medline: 23199171]
11. Willke RJ, Burke LB, Erickson P. Measuring treatment impact: a review of patient-reported outcomes and other efficacy endpoints in approved product labels. Control Clin Trials 2004 Dec;25(6):535-552. [doi: 10.1016/j.cct.2004.09.003] [Medline: 15588741]
12. Weldring T, Smith SM. Patient-Reported Outcomes (PROs) and Patient-Reported Outcome Measures (PROMs). Health Serv Insights 2013;6:61-68 [FREE Full text] [doi: 10.4137/HSI.S11093] [Medline: 25114561]

13. Nelson EC, Eftimovska E, Lind C, Hager A, Wasson JH, Lindblad S. Patient reported outcome measures in practice. BMJ 2015 Feb 10;350:g7818. [doi: 10.1136/bmj.g7818] [Medline: 25670183]
14. Hanssen Rensaa JA, Gligoroski D, Kralevska K, Hasselgren A, Faxvaag A. VerifyMed-A blockchain platform for transparent trust in virtualized healthcare: Proof-of-concept. In: IECC 2020: Proceedings of the 2020 2nd International Electronics Communication Conference. 2020 Presented at: 2nd International Electronics Communication Conference; July 8-10, 2020; Singapore p. 73-80. [doi: 10.1145/3409934.3409946]
15. Hanssen Rensaa JA. VerifyMed - Application of blockchain technology to improve trust in virtualized healthcare services. Norwegian University of Science and Technology. 2020. URL: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2781112/no.ntnu%3Ainspera%3A54255071%3A20647165.pdf?sequence=1 [accessed 2021-10-02]
16. Still B, Crane K. Fundamentals of User-Centered Design: A Practical Approach. Boca Raton, FL: CRC Press; 2017.
17. Anton H. VerifyMed mock-up. Adobe. 2021 Mar 01. URL: https://xd.adobe.com/view/0f333da6-62a5-4928-bb32-b919452ff313-5a60/?fullscreenamp;hints=off [accessed 2021-06-01]
18. Choi YM. Utilizing end User Input in Early Product Development. Procedia Manufacturing 2015;3:2244-2250. [doi: 10.1016/j.promfg.2015.07.368]
19. Brooke J. SUS: A 'Quick and Dirty' Usability Scale. In: Jordan PW, Thomas B, McClelland IL, Weerdmeester B, editors. Usability Evaluation In Industry. Boca Raton, FL: CRC Press; 1996.
20. Fusch P, Ness L. Are We There Yet? Data Saturation in Qualitative Research. TQR 2015 Sep 8:1408-1416. [doi: 10.46743/2160-3715/2015.2281]
21. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences-A scoping review. Int J Med Inform 2020 Feb;134:104040 [FREE Full text] [doi: 10.1016/j.ijmedinf.2019.104040] [Medline: 31865055]
22. Azevedo V, Carvalho M, Costa F, Mesquita S, Soares J, Teixeira F, et al. Interview transcription: conceptual issues, practical guidelines, and challenges. Rev. Enf. Ref 2017 Sep 22;IV Série(Nº14):159-168. [doi: 10.12707/riv17018]
23. Malterud K. Systematic text condensation: a strategy for qualitative analysis. Scand J Public Health 2012 Dec 04;40(8):795-805. [doi: 10.1177/1403494812465030] [Medline: 23221918]
24. Bangor A, Kortum P, Miller J. Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. Journal of Usability Studies 2009;4(3):114-123 [FREE Full text]
25. Legelisten. URL: https://www.legelisten.no/ [accessed 2021-09-27]
26. Dahlin M, Joneborg N, Runeson B. Stress and depression among medical students: a cross-sectional study. Med Educ 2005 Jun;39(6):594-604. [doi: 10.1111/j.1365-2929.2005.02176.x] [Medline: 15910436]
27. Sheard L, Marsh C, O'Hara J, Armitage G, Wright J, Lawton R. The Patient Feedback Response Framework - Understanding why UK hospital staff find it difficult to make improvements based on patient feedback: A qualitative study. Soc Sci Med 2017 Apr;178:19-27 [FREE Full text] [doi: 10.1016/j.socscimed.2017.02.005] [Medline: 28189820]
28. Patel S, Cain R, Neailey K, Hooberman L. General Practitioners' Concerns About Online Patient Feedback: Findings From a Descriptive Exploratory Qualitative Study in England. J Med Internet Res 2015 Dec 08;17(12):e276 [FREE Full text] [doi: 10.2196/jmir.4989] [Medline: 26681299]
29. Deng Z, Hong Z, Zhang W, Evans R, Chen Y. The Effect of Online Effort and Reputation of Physicians on Patients' Choice: 3-Wave Data Analysis of China's Good Doctor Website. J Med Internet Res 2019 Mar 08;21(3):e10170 [FREE Full text] [doi: 10.2196/10170] [Medline: 30848726]
30. Prabhu AV, Kim C, De Guzman E, Zhao E, Madill E, Cohen J, et al. Reputation Management and Content Control: An Analysis of Radiation Oncologists' Digital Identities. Int J Radiat Oncol Biol Phys 2017 Dec 01;99(5):1083-1091. [doi: 10.1016/j.ijrobp.2017.08.015] [Medline: 28939228]

Abbreviations

PREM: patient-reported experience measure
PRO: patient-reported outcome
PROM: patient-reported outcome measure
SUS: System Usability Scale

Edited by G Eysenbach; submitted 24.08.21; peer-reviewed by W Abramson, J Brooke; comments to author 01.09.21; revised version received 02.09.21; accepted 20.09.21; published 22.10.21

Please cite as:
Hasselgren A, Kralevska K, Gligoroski D, Faxvaag A
Medical Students' Perceptions of a Blockchain-Based Decentralized Work History and Credentials Portfolio: Qualitative Feasibility Study
JMIR Form Res 2021;5(10):e33113
URL: https://formative.jmir.org/2021/10/e33113
doi: 10.2196/33113
PMID:

ISBN 978-82-326-6273-9 (printed ver.)
ISBN 978-82-326-6150-3 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

NTNU
Norwegian University of
Science and Technology