Meier, Pascal; Beinke, Jan Heinrich; Fitte, Christian; Schulte to Brinke, Jan; Teuteberg, Frank

Generating design knowledge for blockchain-based access control to personal health records

Information Systems and e-Business Management

Provided in Cooperation with:
Springer Nature

Suggested Citation: Meier, Pascal; Beinke, Jan Heinrich; Fitte, Christian; Schulte to Brinke, Jan; Teuteberg, Frank (2020) : Generating design knowledge for blockchain-based access control to personal health records, Information Systems and e-Business Management, ISSN 1617-9854, Springer, Berlin, Heidelberg, Vol. 19, Iss. 1, pp. 13-41, https://doi.org/10.1007/s10257-020-00476-2

Information Systems and e-Business Management (2021) 19:13–41
https://doi.org/10.1007/s10257-020-00476-2

ORIGINAL ARTICLE

Generating design knowledge for blockchain-based access control to personal health records

Pascal Meier[1] · Jan Heinrich Beinke[1] · Christian Fitte[1] · Jan Schulte to Brinke[1] · Frank Teuteberg[1]

Received: 3 February 2020 / Revised: 15 July 2020 / Accepted: 9 August 2020 /
Published online: 27 August 2020

Abstract

In the course of digitization in healthcare, personal health records (PHRs) are handled as a key solution. Despite the indisputable benefits, the adoption of PHRs is hampered by data security and data privacy concerns. Blockchain technology offers promising potential to address these issues by enabling secure transactions of sensitive data. With regards to PHRs, the blockchain can be used to manage the access to health-related data. Besides existing generic PHR architectures, we systematically identified issues for the healthcare sector that need to be considered for the development of a PHR. We subsequently derived eight meta-requirements that were consolidated into three design principles. Within a 1-year design science research project, we developed the blockchain-secured PHR prototype, OSHealthRec, and evaluated the system in four evaluation cycles. The findings of our research are twofold. On the one hand, we contribute to the design knowledge base by presenting three design principles. On the other hand, we present the development of a real, operational blockchain-secured PHR and the findings from its continuous evaluation, which may serve as useful advice for further solutions.

Keywords Blockchain · Personal health record · eHealth · Design science research

✉ Jan Heinrich Beinke
jan.beinke@uni-osnabrueck.de

Pascal Meier
pascal.meier@uni-osnabrueck.de

Christian Fitte
christian.fitte@uni-osnabrueck.de

Jan Schulte to Brinke
jschultetobr@uni-osnabrueck.de

Frank Teuteberg
frank.teuteberg@uni-osnabrueck.de

[1] Department of Accounting and Information Systems, University of Osnabrück, Katharinenstraße 1, 49069 Osnabrück, Germany

1 Introduction

While various industries benefit from the opportunities offered by digitization, the healthcare sector continues to face challenges in implementing these in a targeted and broadly supported manner. This is particularly important in the exchange of patients' data, as many healthcare stakeholders rely on accurate information about previous treatments to provide the best possible care (Poston et al. 2006). Information Systems can enable fast and accurate communication, which modernizes today's healthcare processes where medical reports are primarily sent by post and coordination usually takes place by telephone or fax (Foronda et al. 2016). Personal health records (PHRs) have the potential to substantially improve communication in healthcare such that authorized stakeholders have immediate access to patient health data in real time (White and Danis 2013). This would significantly reduce misunderstandings, redundant examinations, adverse drug events and delays in treatment (Chao et al. 2013). In addition, the transparent access to personal health data might increase health awareness of the patient (Meier et al. 2019). Given their numerous advantages, PHRs have been established in many countries worldwide, such as the Netherlands, USA, Canada New Zeeland, Estonia and Scandinavian countries (Al-Aswad et al. 2013; Amelung et al. 2016). In contrast, the adoption of PHRs in other developed countries, e.g. Germany, is hampered by data privacy and data security concerns (Hoerbst et al. 2010; Nohl-Deryk et al. 2018; Adelmeyer et al. 2019). The anxiety associated with unauthorized persons gaining access to sensitive patient data through security breaches is regularly confirmed by hacker attacks on PHR providers (Healthcare-IT-News 2018; Gillum et al. 2019; Kerkmann and Micijevic 2019).

Similar to the healthcare industry, the financial sector handles sensitive and private data that must be effectively protected from unauthorized access, manipulation and misuse. Since Nakamoto introduced Bitcoin in 2008, blockchain technology has gained tremendous popularity in various fields of application (Nakamoto 2008; Beck et al. 2017). In particular, blockchain technology improves the traceability of transactions and contributes to disintermediation, thus strengthening the required trust between (business) partners in their shared transactions and data (Weber et al. 2016; Rückeshäuser 2017). Given the decentralized system and consensus mechanism, each transaction is unchangeably recorded. Blockchain was subsequently discussed as a promising solution in the healthcare environment as well (Mettler 2016). Estonia, as a pioneer in digitization—especially e-government—already implemented an EHR in 2008. Eight years later, the Estonian eHealth Foundation started a new era in securing healthcare data by safeguarding off-chain stored EHRs using blockchain technology that logs all data access activities (Einaste 2018). The blockchain ensures that users own and control their personal data. Our system respects the fact that the user owns the data and only gives access to the data to healthcare professionals after approval by the user. The access control is fine-grained, thus strengthening compliance with data privacy and data security. For example, users can revoke access authorizations at any time or grant one-time access only. Moreover, the accesses are logged transparently and traceably.

However, since the legal and organizational requirements of healthcare systems are highly heterogeneous in different countries, existing solutions are not unrestrictedly transferable into other healthcare systems. In addition, an EHR requires healthcare institutions to administrate the data. By using PHRs and by considering open standards and interfaces, both patients and healthcare providers can continue to use their own familiar systems. Various generic architectures have been suggested in the scientific literature in the healthcare informatics and information systems domain (Roehrs et al. 2017; Ekblaw et al. 2016). However, to the best of our knowledge the generation of design principles (DP) and recommendations for a blockchain-secured PHR are currently missing. This motivates us to address the following research question (RQ) in order to make design knowledge for blockchain-secured PHRs applicable and transferable:

RQ: How can a patient-centered blockchain-secured PHR that stores health related data and is managed by the patient be designed and evaluated regarding user's acceptance?

To answer the RQ, we conducted a systematic literature review to identify relevant issues. These issues were consolidated into meta-requirements (MRs) and transformed into three DPs. We subsequently considered the DPs by developing the PHR *OSHealthRec* which manages the authorization and access rights via a blockchain and stores the data off-chain within a 1-year research project. The system was evaluated in four iteration cycles with three feedback loops to achieve the best possible user acceptance.

Our findings reveal relevant insights for research and practice. The systematic development of three DPs as well as the findings from our evaluation cycles may serve as valuable knowledge for further developments (Gregor and Jones 2007; Beck et al. 2016). Moreover, the medical practice and decision-makers for the implementation of PHR systems gain substantial insights into the potentials of user-centered blockchain-secured PHR solutions.

2 Background and related work

2.1 Evolution of personal health records

In the scientific literature, as well as in practice, there are numerous different terms for PHRs (Angst et al. 2006; Al-Aswad et al. 2013; Heart et al. 2017). In the comparison of international literature in particular, various terms are used for the same concepts, and the same terms are simultaneously used for different concepts (Haas 2017). Therefore, this chapter defines the evolution of PHRs and which conceptual understanding of a PHR is the basis of our research.

First, a distinction must be made between *patient records* and *personal health records*. Patient records are administrated by healthcare professionals and usually imply that someone is ill and/or has a treatment within a healthcare institution. The

initial type of *electronic health record* (EHR) was the digital storage of patient-related documents within an institution, for example by scanning medical reports (internal electronic patient files). In the context of increasing cooperation between healthcare professionals, patient data should be stored in electronic files that can easily be shared across institutions in the next step (cross-institutional electronic patient records). However, each patient record still implies that a person is having a treatment in at least one healthcare institution.

In contrast, a *personal health record* is administrated by the user him- or herself and does not require any institutional treatment or therapy (Burrington-Brown et al. 2005). Without having health-related issues, users can track their health status and health-related data, and they can pursue health prevention. In addition to professional health data, users can store wellness data, such as vital signs, measured by wearables (Gay and Leijdekkers 2015; Meier et al. 2019). Apart from the advantages of data sovereignty and self-determination, a patient-centered health record causes problems with regard to data quality and completeness of the record. Patients have the opportunity to conceal important information because they might feel uncomfortable about it and cannot assess the relevance of this information for other potential treatments (Tang et al. 2006). Typical examples of withheld information are infection with AIDS or the use of Viagra, which could be kept secret because patients might feel ashamed. Nevertheless, patient-centered health records appear to be better accepted by patients, who seek more self-determination with regard to their health-related information (Klecun 2016).

The advantages of a PHR are its continuous availability; time-, location- and device-independent access; and increased transparency (White and Danis 2013; Haas 2017). To date, many healthcare systems are comparable to a black box, to which only healthcare professionals have access (Busse et al. 2013); usually patients only have access to their own data on request. Presuming that the data are safe and protected against manipulation, a PHR contributes to better involvement of the patient in his or her healthcare treatment. This increased empowerment can motivate him or her to better comply with therapy instructions. In addition, PHRs support efficient communication and information exchange, and they avoid redundant treatments, which enable time and cost savings for healthcare systems (Chao et al. 2013; Haas 2017).

2.2 Blockchain in healthcare

Given the advantages of blockchain technology, including being tamper-proof (Risius and Spohrer 2017; Kumar and Mallick 2018), a strengthening in required trust in transactions between (business) partners as well as the permanent traceability of transactions (Swan 2015; Weber et al. 2016; Rückeshäuser 2017), its use is currently being discussed, field-tested and evaluated in various sectors (Beinke et al. 2018; Friedlmaier et al. 2018). These advantages make blockchain particularly attractive for healthcare scenarios in which highly sensitive patient data are transmitted. However, there are also challenges, for example in terms of data protection. In the health sector in particular, extremely sensitive personal data is collected, stored

and processed. With the General Data Protection Regulation (GDPR), the European Union has adopted a comprehensive set of data protection regulations. For example, articles 17 and 18 of the GDPR[1] guarantee the right to delete or modify data. Furthermore, the GDPR contains explicit guidance on the handling of health data (e.g. articles 35, 45, 53, 54, 55).[2] The right to modify or delete data would not be feasible with a blockchain that stores the data in a tamper-proof manner. Therefore, we have decided to use off-chain data storage and thus follow the recommendation of the European Parliamentary Research Service (Finck 2018). The off-chain storage of personal data enables us to delete (or modify) data. By using a private blockchain we deliberately restrict the circle of blockchain operators. Potential operators in this case would be, for example, a consortium of doctors' and pharmacists' associations and health insurance companies.

Various researchers, such as Linn and Koo (2016), Mettler (2016), Stagnaro (2017), Gordon and Catalini (2018) and O'Donoghue et al. (2019), have investigated the potentials of blockchain use cases in health, IT and healthcare-related research. Rono (2016) developed, implemented and evaluated an eHealth interoperability platform for Nairobi health facilities to enable fast and secure data exchange between healthcare stakeholders. Kuo et al. (2017) identified explicit use cases for blockchain in healthcare and derived the key benefits of improved medical record management, enhanced insurance claims, accelerated clinical or biomedical research and advanced biomedical or healthcare data ledgers. Apart from the high potential, the authors also identified key challenges such as transparency and confidentiality, speed and scalability, and the threat of a 51% attack.

Further research focused on the use of blockchain technology to secure PHRs, such as studies by Roehrs et al. (2017), da Conceicao et al. (2018), Dagher et al. (2018) and Beinke et al. (2019). Leeming et al. (2019) identified 11 solutions for blockchain PHRs, five of which—Guard Time, Carechain, Dovetail, MedRec and Medical Chain—are published in Whitepapers. So far, only a few approaches have been implemented and evaluated, such as OmniPHR by Roehrs et al. (2017), MedRec by Ekblaw et al. (2016) and FHIRChain by Zhang et al. (2018).

2.3 Best practices of blockchain-based personal health records

Medrec is a blockchain-based EHR on the basis of Ethereum smart contracts (Ekblaw et al. 2016). The system provides comprehensive information to a patient and allows for integration into existing information systems by healthcare professionals. The authors claim that Medrec constitutes a proof of concept about the ability of blockchain to secure medical information within an interoperable environment and to increase transparency in healthcare (Ekblaw et al. 2016).

[1] https://gdpr.eu/tag/gdpr/.

[2] Similar to the regulations in the European Union, the USA also has special data privacy regulations regarding the handling of health data, for instance the Health Insurance Portability and Accountability Act. https://www.cdc.gov/phlp/publications/topic/hipaa.html.

OmniPHR Roehrs et al. (2017) present the development, prototype implementation and evaluation of the blockchain-based OmniPHR, which works with the interoperability standard openEHR. Systematic evaluation with a performance experiment revealed three major findings: (1) the combination of the "openEHR standard with the blockchain technology created a unified and interoperable view of health data." (Roehrs et al. 2017); (2) the Chord algorithm for data replication seems to offer a more efficient and scalable solution than using cryptocurrency platforms, which is an essential benefit for an area-wide and uniform solution; and (3) an empirical evaluation demonstrated an adequate network-level performance of OmniPHR. Overall, the authors propose the use of blockchain to effectively integrate PHRs for a large number of patients by considering interoperable health data standards.

FHIRChain Zhang et al. (2018) systematically identified the requirements and their implications for a blockchain-based PHR to share clinical data and accordingly developed an architecture for the FHIRChain. The system was subsequently evaluated within a case study of collaborative decision-making for remote cancer care. The key findings were that FHIR provides "trustless, decentralized storage for necessary meta information and audit logs" (Zhang et al. 2018). Moreover, the system enables fast data exchange without necessary uploads and downloads and the maintenance of access rights.

In addition to prototype solutions from research projects, Estonia, which is one of the pioneers of the digitization of public services, is using a productive blockchain-based EHR. A nationwide EHR was already established in 2008, and in 2016, the country launched a new EHR using KSI blockchain technology (e Estonia 2020; Guardtime 2020). It is organized such that every physician potentially has access to all available PHRs. All access is unchangeably tracked in the blockchain, and if a patient detects unauthorized access by any physician, he or she can report this at a complaint office. In case of unauthorized use, the physician can lose his or her approval.

To accelerate the use of blockchain in healthcare, more research on design knowledge is necessary to validate the currently limited results. This motivates us to analyze the requirements for a blockchain-secured PHR, implement the solution in an operational prototype and subsequently to evaluate the prototype in a multi-methodological and iterative research approach.

Within the scope of our research we define a blockchain-secured PHR as a patient-centered platform that stores health-related data. The authorization and access management is unchangeably traced in a blockchain to avoid manipulation or misuse. In this approach the content is efficiently stored in an off-chain database while the access is secured by a blockchain (Esposito et al. 2018). In contrast to the Estonian model, healthcare professionals can only access the PHR with permission of the patient. However, once someone get access he or she can see the complete medical record. This avoids the above mentioned problem, that patients may hold back relevant information.

3 Research approach

In the course of eHealth evolvement, new interdisciplinary research fields such as health informatics were established to successfully implement technology in the healthcare sector. However, the systematic assessment of requirements, the construction of architectures and the development of prototypes remain the core competences of information systems research. In the information systems discipline, the development of research artifacts, such as our blockchain-secured PHR, is often conducted by following the design science research (DSR) paradigm proposed by Hevner et al. (2004). In addition to a rigorous use of methods and theories from the knowledge base, a constant exchange with the application domain ensures the relevance of the artifact. Holmström et al. (2009) point out in their contribution that in the DSR paradigm the knowledge base is expanded if either existing kernel theories are reviewed with existing IT artifacts or new artifacts are developed. Our contribution can be assigned to the latter. Through our approach we first develop a prototype and at the end of the article we draw conclusions about possible theoretical implications. Following the approach of Beck et al. (2016), we argue that currently available blockchain applications are still rare. Nevertheless, first applications demonstrate the potential of blockchain technology, e.g. it is possible to establish trust between transaction partners (in our example: doctor and patient) and to reduce transaction costs by a digital blockchain-based solution. To test such theories, however, functioning prototypes are required. Therefore, in this paper we present a prototype, built upon our derived design principles for blockchain-secured PHRs, which can be used by other researchers as well as practitioners.

For a structured implementation, Peffers et al. (2007) transferred the design guidelines into a six-phase iterative methodology, which was used as a framework for the design of our prototype. To identify the related work from science and practice and to elaborate the existing problems and solutions in the domain, a systematic literature review and a market analysis were carried out in the first iteration. We conducted the literature review according to Webster and Watson (2002) and vom Brocke et al. (2009). Given the implementation of the first blockchain-based application (Bitcoin in 2008), the period to be investigated was set at 2008 onwards (Nakamoto 2008). Within this period, we searched the *EBSCOHOST*, *AISeL*, *Google Scholar*, *Sciencedirect and Springerlink* databases with the following search string: (“personal health record” OR “electronic health record”) AND (“blockchain” OR “distributed ledger”). Since insights from EHR research may also affect PHR systems, we included EHR into our literature review. After filtering the contributions by abstract and title, and with subsequent evaluation of each paper’s relevance for our study and a forward/backward search, we included 52 papers in our analysis. The market analysis was carried out to identify and analyze existing applications in the field of blockchain-based EHRs and PHRs. For this purpose, we performed an open search with Google and the startup databases CrunchBase[3] and Angellist.[4]

[3] www.crunchbase.com (Accessed 19 June 2020).

[4] www.angel.co (Accessed 19 June 2020).

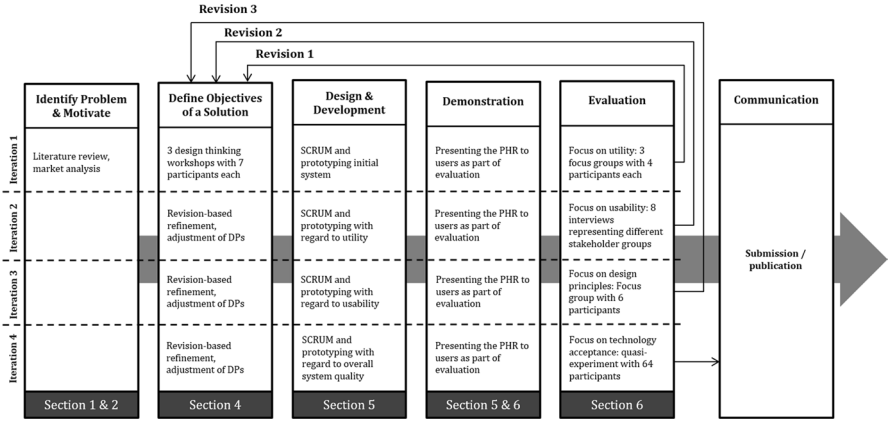

Fig. 1 Research approach and structure of this contribution

During the entire development, the market was regularly screened for additional (new) applications.

With the results of the literature review and market analysis, three design thinking workshops were held (Plattner et al. 2009), each with seven participants from the fields of computer science, information systems and healthcare, and the initial issues and MRs for the blockchain-secured PHR were elaborated in these sessions. Derived from the MRs, a first draft of the DPs was defined. The DPs guided the development of a first prototype, by using SCRUM and prototyping (Dey et al. 2001). This prototype comprised the functional scope of the blockchain-secured PHR, consisting of a unified database with the associated blockchain, web services for interaction with this database and a web platform for the various stakeholders (doctors, patients, employees). During the first evaluation, we presented the system to the participants. Multiple scenarios (e.g. saving documents, data queries by the physician) were presented from the perspective of the individual stakeholders. The research approach including the individual steps is summarized in Fig. 1.

4 Derivation of design principles for blockchain-based access control to personal health records

Based on our literature review, we identified issues (Is) regarding the use of PHRs. The issues result in requirements, which were summarized in meta-requirements (MRs). In the next step the MRs were consolidated in initial design principles (DPs) for the development of a blockchain-secured PHR.

Digitalization and the use of information technology have fundamentally transformed the healthcare sector (Feldman et al. 2018). The dissemination of technology is accompanied by a variety of different systems (I1) (Dugas et al. 2016). Healthcare systems are especially characterized by a great heterogeneity of information systems for different stakeholder groups such as hospitals, doctor's offices, pharmacies,

insurances, laboratories, therapists and care services. To ensure data compatibility, a PHR must be able to be integrated into the existing information systems (MR1), and the integration should consider the high heterogeneity of the data (I2) (Oemig and Blobel 2014). Particularly data must be structured and harmonized within the PHR (MR2) (Veseli et al. 2012). Therefore, the requirement for the internal structuring and standardization of data as well as the integration of a PHR into existing systems results in the following DP:

DP1: Provide the PHR with a unified data structure, which delivers the data via interfaces to all involved systems. Therefore, the PHR integrates easily into an existing digital health ecosystem.

With a unified data structure, it is possible to share the data almost error-free with different systems. However, the risk exists that the data may be manipulated (I3) from the outside, primarily because of unauthorized access to the data (I4) (Nohl-Deryk et al. 2018; Gillum et al. 2019). As a result, a PHR relies on a secure and reliable infrastructure (MR3) that is supported by clearly defined authorization and authentication mechanisms (MR4) and a detailed and adaptable role concept (MR5). In the case of data manipulation, there is often no access tracking and modification history (I5), which is why the PHR must have traceability mechanisms (MR6).

DP2: Implement the PHR on a safe and reliable infrastructure with traceability mechanisms. This ensures that sensitive data cannot be accessed without permission and that misuse can be traced back.

Current health record systems are mostly exclusive to the healthcare professionals. In addition, PHRs are in an early stage of development, and the adoption is consequently not yet far advanced. As a result, few PHRs are available to citizens (I6), and the reception of patient health data remains delayed (I7). Furthermore, because of the lack of user experience with a PHR, it must be designed in a user-centered way to achieve high acceptance (MR7) (Tavares and Oliveira 2016). MR7 is also supported by the fact that the existing PHRs do not provide sufficient opportunities for users to control rights over stored documents for healthcare stakeholders such as doctors and pharmacists (I8) (Seitz and Wickramasinghe 2017). One of the reasons for the insufficient assignment of access rights is that users find it difficult to use PHRs (I9). From I8 and I9, it follows for MR8 that the interface should be information-focused so that users know to whom they are granting rights to their health data.

DP3: Provide the PHR with an easy-to-use and information-focused interface with comprehensive authorization mechanisms. Users can then deliberately determine who has access to their personal health information.

Figure 2 summarizes the connections between issues, meta-requirements and initial design principles.

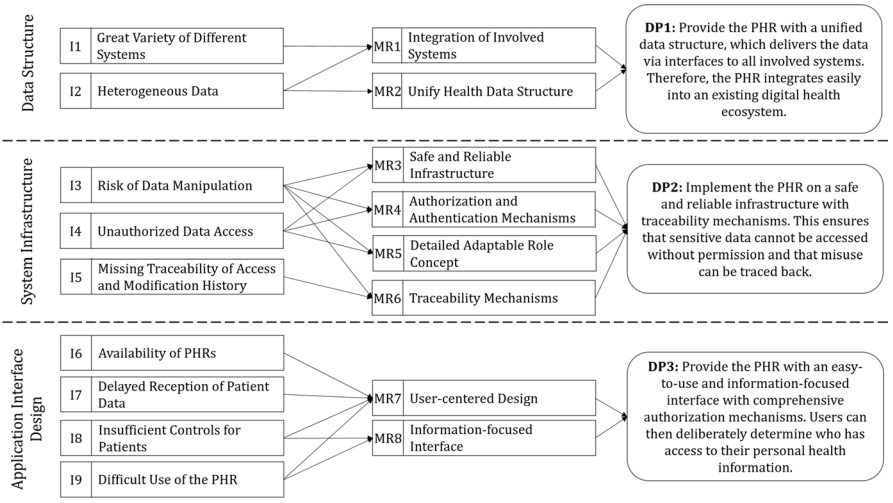

Fig. 2 Issues, meta-requirements and initial design principles for blockchain-secured PHRs

5 Blockchain-based access control to personal health records

5.1 Use case

Section 2 discussed the current use of PHRs in healthcare and the use of blockchain technology to improve the traceability of access to PHRs. Since the development of a PHR for the entire healthcare system is too extensive in the first place, the development of our prototype will initially focus on the communication between the treating doctors, their associated employees and the patients.

For this purpose, our PHR OSHealthRec manages patients' documents. To do so, both the patient and the attending physician need a personal account. The patient provides access to his or her personal health information by scanning his or her attending physician's individualized QR code. This ensures that both the physician and the patient agree to the authorization. The physician and his or her employees can then upload treatment reports and other files to the patient's account, and the patient is able to continuously track his or her treatment record. To ensure the security of the therapy, the patient can only read the documents but cannot change them or upload his or her own files. All process regarding access management are carried out via blockchain. The documents are stored outside the blockchain, as it would otherwise become too large and inefficient. When accessing and storing files, the blockchain provides the user with the access information (Esposito et al. 2018).

5.2 Data structure and system architecture

At the beginning of the development in December 2018, the choice for a blockchain was limited to a few providers, including Hyperledger, R3Corda and Ethereum, and

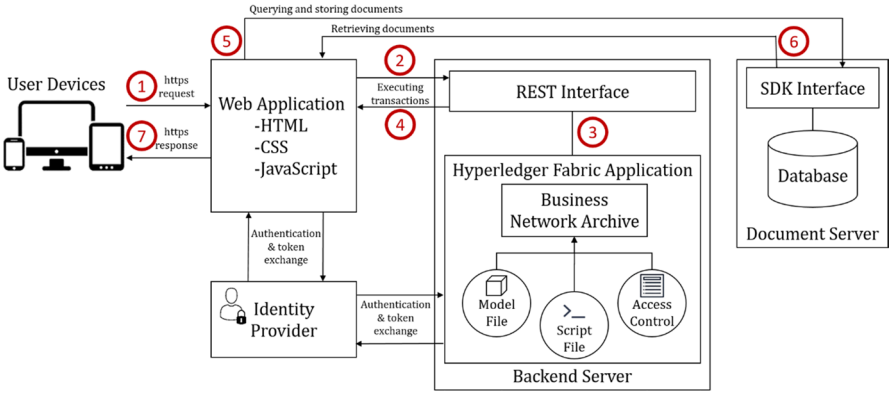

Fig. 3 System architecture for OSHealthRec

that choice was made based on the following criteria: functional extent, support, cost and interfaces. We finally chose Hyperledger Fabric and Hyperledger Composer, which are part of the Hyperledger Project founded by the Linux Foundation and is intended to develop enterprise applications based on a private blockchain. It is based on a modular system that offers different components, such as services for membership or ordering (Sousa et al. 2018). With Hyperledger Composer a business network consisting of participants, assets, access controls and transactions can be formed. Participants and assets are defined with their attributes in a model file. Based on the model file, the transactions between participants and assets in the business network are described using JavaScript. The access controls are used to define the access rights of participants to assets, transactions and other participants. These components are then used to create the business network archive, which can be published on an existing Hyperledger Fabric instance.[5]

Hyperledger Composer does not offer sufficient possibilities to save documents (e.g. medical reports). Therefore, the Hyperledger Fabric application must be supported by a separate off-chain storage. For this purpose, a system extension was created to manage the documents. The blockchain application is used to manage the path to the file, with which the corresponding document can be retrieved from the system. To enable the user to easily interact with the PHR, a web application was developed that can call up the functions of the application via REST services. Through implementation of a responsive web application, it is possible for every browser-enabled device to retrieve the data and to visualize the information in an attractive way. An external identity provider (e.g. GitHub or Google) handles the authentication for the web application as well as the Hyperledger application. The described architecture is illustrated in Fig. 3. General information about the participants and the assets is communicated and maintained directly with the Hyperledger

[5] https://hyperledger.github.io/composer/latest/introduction/introduction.html (Last accessed 19 June 2020).

Fabric application, and each report is stored as a document. Therefore, every user can store and access the reports, so that the prototype addresses DP1. To store and retrieve documents, the corresponding transaction is first initiated in the Hyperledger Fabric application and checked for authorization. Afterwards, the access path via which the document is requested from the document server is shared. This process is represented by the red circled numbers in Fig. 3. First, the user sends a request to the web application (1) which queries the Hyperledger API (2); then, the Hyperledger Fabric application checks the eligibility of the transaction and executes the transaction with the necessary permission (3). Thereafter, the API answers the request with the respective access path (4), and with this information, the web application which is authenticated for access to the document server retrieves the data from the document server (5, 6). Finally, the web application makes the documents available to user via a link with an access token so that they can view the document (7).

To create the model file that describes the participants and assets, the first step was to identify the actors in the use case and to represent them using a UML class diagram (Fig. 4a). In total, three classes of actors are involved in the use case: patients, doctors and employees. Accordingly, there is the abstract class *Person*, which defines the key attributes of a person, such as birthday and name. For *Patients*, this class is used to record treatment-related data as well as the verified doctors and uploaded reports. In addition, patients can add or delete the access permission to doctors and their employees. For *Doctors*, information about the medical practice and the medical specialty is recorded. In addition, the system records which employees work for the doctor, who retrieves which data and which patients are treated by which doctor.

The doctors can provide reports for the patients and add or delete staff and patients. For example, one employee can work in a shared office for multiple doctors. We considered this by adding an employee attribute that indicates the doctor for whom he or she works, and employees can add reports to patients on behalf

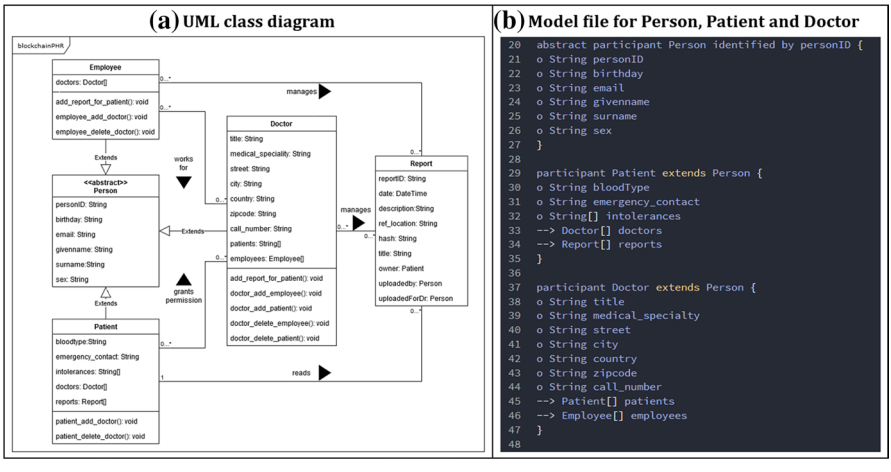

Fig. 4 UML class diagram and model file

of the doctors as well as add or delete doctors. The reports that can be added by doctors or employees have an ID, creation date, title, description and details for and by whom the report has been uploaded. The *ref_location* additionally specifies the path to the report in the document system, since the report should not be saved in the blockchain. Storing the reports directly in the blockchain increases its size significantly. Moreover old versions of the documents would remain immutable in the blockchain even if changes are made (Finck 2018). This would violate privacy regulations such as GDPR. For example, the transfer of the *Person*, *Patient* and *Doctor* classes, described in the UML class diagram, into the format of the participants is illustrated in the model file in Fig. 4b.

The functions defined in the UML class diagram are defined as transactions in Hyperledger Composer via the script file. Figure 5a depicts the function *add_report_for_patient*. The required parameters are passed to the function. The first step checks whether the report has already been made available to the patient. The report for the patient is then added, and the patient is updated in the application. Since the function *add_report_for_patient* may only be executed by doctors and employees, the rules must be defined in the access control. Figure 5b displays the rules for the doctor. For this purpose, the rule *DoctorAddReportForParticipantTransaction* specifies that all participants of the type *Doctor* have permission to create the transaction *add_report_for_patient*. Within the rule *DoctorAddReportForPatient*, the doctor is then allowed to make a change using the transaction within the participant of the type *Patient*, if the doctor has been defined as the treating doctor.

(a) script file defining transactions and functions

```
async function add_report_for_patient(arfp){
  let reportArray = arfp.patient.reports;
  // Check whether the report already exists in the array
  let index = reportArray.indexOf(arfp.report);
  if (index > -1) {
    return;
  } else {
    // Add report to array
    reportArray.push(arfp.report);
    // Write update to database
    let participantRegistry = await getParticipantRegistry('org.oshealthrec.network.Patient');
    await participantRegistry.update(arfp.patient);
  }
}
```

(b) access control defined by rules

```
// Rules to allow the doctor to add a report to the patient's reports array
rule DoctorAddReportforPatientTransaction {
  description: "Allow doctor to create add_report_for_patient transaction."
  participant: "org.oshealthrec.network.Doctor"
  operation: CREATE
  resource: "org.oshealthrec.network.add_report_for_patient"
  action: ALLOW
}

rule DoctorAddReportforPatient {
  description: "Allow doctor to write report into his patient´s reports array."
  participant(p): "org.oshealthrec.network.Doctor"
  operation: UPDATE
  resource(v): "org.oshealthrec.network.Patient"
  transaction(tx): "org.oshealthrec.network.add_report_for_patient"
  // Search the patient's doctors array for the Doctor
  condition: (
    v.doctors.some(function (doctor) {
      return doctor.getIdentifier() === p.getIdentifier();
    })
  )
  action: ALLOW
}
```

Fig. 5 Script file and access controls

The described architecture and implementation of the Hyperledger Fabric application ensures that the healthcare actors and patients communicate the reports securely. Every access and retrieval is stored within the application by the blockchain, and it is possible to trace and, if necessary, retrace every interaction. In this way, we addressed DP2 in our prototype.

5.3 Application interface design

For secure use of the PHR, it is essential that users know how to correctly use the system (Tavares and Oliveira 2016). The screenshots in Fig. 6 illustrate how the interface was designed considering DP3. The aim was for users to be able to easily interact with the system and be confident in administrating access rights. This ensures that users always know who is allowed to provide reports and who has access to the information therein.

Since the individual groups of actors require different functions, the web interface provides a separate view for each group. The access works via a common login page. During the login process, the system checks the group to which the user belongs; then, the user receives the respective view of his or her group. For each view, the user's personal information is displayed first. The different views are described next. Figure 6a, b depict the views of the patients. In addition to the profile, there are menu items titled *Documents* and *Approvals*. Under the menu item *Documents*, illustrated in Fig. 6a, all reports of the patient are listed in tabular form.

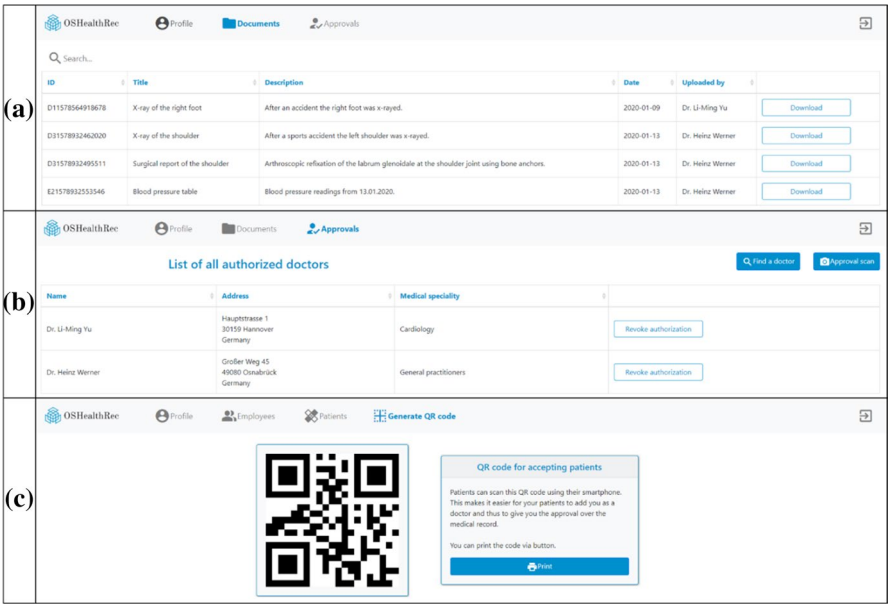

Fig. 6 User interfaces of the prototype. **a** Patient document view, **b** patient approval view and **c** doctor's QR code generation view

The ID, the title, a short description, the creation date and the responsible physician are displayed. Via a button, the corresponding document can be downloaded, and using a search function, patients can filter the documents in the individual categories according to search criteria.

The *Approvals* tab, presented in Fig. 6b, lists all physicians to whom the patient has already granted access to his or her data. The title, name, address and specialization of the respective doctors are displayed here. Furthermore, the permitted authorization to the individual doctors can be revoked, and the user has the option to grant further doctors permission to access their data under this tab. Patients have two options for this. First, with the manual search, all physicians in the system are listed, and using a search function, users can search for the corresponding physician and grant him or her access to their accounts. Second, by means of the share scan, a doctor's QR code can be scanned via the camera of the device; this automatically gives the doctor access to the patient.

The doctor's view includes the following four tabs: *Profile*, *Staff*, *Patients* and *Generate QR Code*. Under *Staff*, all employees of the doctor are listed with name and date of birth. In addition, further employees can be added, or existing employees can have their authorization withdrawn.

The patient's tab lists all patients who granted the doctor permission to access their reports, together with their key information. By choosing a patient, the physician can access the overview of the respective patient with information about the person and all reports. In addition, the doctor can create new reports for this patient. The *Generate QR Code* tab, depicted in Fig. 6c, displays a QR code with the associated doctor's ID. This QR code can be printed out to subsequently pass on to new patients for easier approval.

6 Evaluation

Within the design process, four major evaluation cycles were carried out. All evaluations were conducted according to the design cycles as described in Sect. 3. The continuous evaluation essentially serves to ensure continuous improvement and to eliminate identified weaknesses as quickly as possible. The formative evaluation of the prototype was divided into four cycles with different focuses and respective methods according to Table 1 (Venable et al. 2016).

Table 1 Overview of evaluation cycles

No	Focus	Method	No. of participants
I	Utility	Three focus group workshops	4 each (12 in total)
II	Usability	Expert interviews	8
III	Design principles	Focus group workshop	6
IV	Acceptance	Survey	64

In the first evaluation cycle, focus groups were asked to perform certain tasks with the PHR. These tasks were embedded in scenarios; for example, incorrectly entered X-ray images were to be replaced by new (correct) ones. The scenarios aimed at testing all functionalities of the application from the perspectives of all involved stakeholders (patients, doctors and employees). The participants in the focus groups were experts from the IT and healthcare sectors. The subsequent group discussions followed few and open guidelines, and they were recorded, transcribed and analyzed. In general, a focus group has the advantage of making it more difficult for participants to provide a desired answer. Instead, they must debate with one another and try to explain their own impressions, opinions, feelings and ideas and eventually convince other participants (Lune and Berg 2017). With the overview of the system, the participants evaluated the prototype in the first iteration regarding its utility. This ensured that the prototype did not lack any important functionalities for the use case. Therefore, three focus groups, each with four participants, were conducted. Each focus group attempted to gather experts from different fields to evaluate the solution from different perspectives. The results of the evaluation were used to expand the system in the second iteration. First, the MRs and DPs were revised, and the prototype was further developed analogous to the procedure of the first iteration. With the adapted range of functions, the prototype was evaluated in the second iteration with regard to usability. Eight expert interviews with future patients were conducted to ensure that the solution meets users' requirements. Through the interviews, further necessary adjustments to the solution were identified, and they were implemented in the third iteration after adaptation of the MRs and DPs. This iteration was concluded with an evaluation of the implementation of the DP in a focus group with eight participants. The evaluation revealed that the DPs were sufficiently considered in the solution. Finally, the system was evaluated through a survey with regard to its acceptance by future patients. Based on the positive evaluation of the prototype, no further adjustments regarding the DPs and the prototype were identified.

I. Evaluation cycle: utility

In the first evaluation cycle, some features of our prototype were positively highlighted. These included the possibility to access all information and data at any time without additional effort (e.g. searching for the treating physicians) and the associated traceability of the history as a useful benefit. This highlights the advantages of providing all information to healthcare professionals by default. Only if a patient actively wants to constraint information, e.g. in order to receive a second independent and unbiased opinion, he or she should be given the opportunity to block a report or diagnosis.

More information, such as the specialization of the physician or the position of an employee in the organization, was desired by the participants. Furthermore, the name of the doctor's office or hospital, along with information about the last visit to the doctor and current complaints, is missing in the patient's profile. According to the participants, it would also be helpful to include the physicians who are no longer approved, in order to trace the history of the treatment even better. We recommend

future PHR provider to enrich every uploaded entry with detailed meta data, e.g. the author's contact data. In addition, the participants wished for a more thorough sorting of the information or data in the file. A practical recommendation was the subdivision of the documents into, for example, reports and images. However, other participants perceived the structure of the document list as convenient. Moreover, the recognized document standards in the medical field must be considered. Overall, the loading time was evaluated as critical for the future use of such a PHR. Within the scope of further development, it was possible to address the technical challenges in particular (improvement of loading times, subdivision into various document types) as well as the finer division of information (e.g. appointment or treatment history).

II. Evaluation cycle: usability

Similar to the first evaluation cycle, the insufficiently detailed information provided by the actors in the prototype was again critically discussed. More information, such as the profession of the doctor or the position of employees in the organization, was desired. Furthermore, the interviews revealed that the use of the QR code is not intuitive—finding the scan function and saving the code in particular caused problems for the participants. Moreover, given the missing specialization of healthcare professionals, the participants criticized the process of searching for a doctor for being confusing. Then, with regard to the loading time, which was negatively noted in the first cycle, it was improved adequately, such that it was no longer mentioned as a critical issue. The feedback regarding the performance confirmed that off-chain storage of health data and blockchain-secured access management provides the best combination of security and efficiency. In addition, the interviewees valued the clearly arranged user interface and its intuitive use. As a result of the responsive web design of the application, mobile use was also positively evaluated. For further improvement, it was stated that additional icons should be added to the existing text elements to make the user experience even more appealing and intuitive. We recommend PHR providers to ensure an intuitive use by presenting the features with distinctive icons.

During the interviews, possible functional enhancements were discussed. Some ideas for future extensions, such as a QR code on the medical card or geographically related searches, were mentioned. However, these were not taken into account, since we developed a prototype in the first place to demonstrate the feasibility of blockchain technology for PHRs. Future implementations of PHRs should consider these recommendations.

III. Evaluation cycle: design principles

Throughout the first two evaluation cycles, the initial design principles were refined. In order to ensure that the DPs are precisely formulated and that the prototype reflects them, the focus group critically reviewed both. Questions and concerns about the rights of the actors (e.g. in the release process) were discussed in depth. With the help of the rules in Hyperledger Composer, an authorization and authentication procedure was subsequently implemented. Thus, during the login process, the role and rights of the user are checked. This prevents insufficient

data sovereignty and enables an adaptable and detailed role concept, and errors or deliberate manipulations by unauthorized users are prevented. Moreover, the rules of the prototype guarantee the assignment of information to the correct target person. Furthermore, the arrangement of design elements was discussed, and their use on mobile devices in particular was positively emphasized.

In addition, the DPs were formulated according to Gregor et al. (2020) to take into account important components such as *aim*, *implementer*, *context*, *mechanism* and *rationale* and to transfer them into a structure that enables researchers as well as practitioners to incorporate them into their own work. After the revision, the workshop concluded that the DPs were successfully applied in the prototype, so that the prototype can be evaluated for user acceptance. The final DPs are presented in Table 2.

IV. Evaluation cycle: user acceptance

A survey was conducted during the last evaluation cycle. The technology-acceptance model (TAM) (Davis 1986) served as the theoretical basis—perceived ease of use (PEOU), perceived usefulness (PU) and intention to use (ITU)—which was supplemented by three further constructs, namely, privacy (PR), security (SE) and control (CO) (Davis 1986, 1989). Both the constructs and the underlying items were systematically derived from the literature (see "Appendix"). The decision to extend the TAM with the privacy, security and control constructs was based, on the one hand, on the fundamental considerations of improving security (and privacy) through blockchain technology and, on the other hand, on the feedback from the previous evaluation cycles, to afford the user full control over the system and his or her own data (control).

Prior to the survey, the respondents received an introductory text describing the current challenges and opportunities of digital patient records. They were also provided with a link to the blockchain-secured PHR developed by us, and they were asked to test it in detail from the perspectives of a patient, a doctor and an

Table 2 Design principles for blockchain-secured PHRs

#	Design principle specification
DP1	To allow PHR providers to enable users such as patients and healthcare service providers and their systems to access and communicate patient's health data within any existing system architecture ensure a unified data structure, which provides the data via interfaces to all involved systems, because the adaptable and easy-to-integrate architecture supports the broad adoption of the PHR in healthcare services
DP2	To allow PHR providers to enable PHR users such as patients and healthcare service providers to safely and reliably access and communicate patient's health data within the PHR ensure by usage of a blockchain with well-defined data, access and role models that every access to patient's health data is authorized because managing access rights and tracing transactions strengthens data security and records as well as prevents misuse
DP3	To allow patients to deliberately determine access permission to their personal health information during the whole interaction with the PHR provide the PHR with an easy to use and information focused interface with comprehensive authorization mechanisms, because the safe interaction enables the user to self-manage his or her PHR reliably

Table 3 Reliability and validity

Factor	CA	CISC	IIC	CR	AVE
Privacy	0.863	0.691–0.783	0.667	0.916	0.784
Security	0.763	0.501–0.745	0.512	0.864	0.682
Control	0.778	0.530–0.749	0.550	0.876	0.702
Perceived ease of use	0.947	0.869–0.911	0.862	0.967	0.908
Perceived usefulness	0.770	0.545–0.663	0.532	0.866	0.683
Intention to use	0.804	0.668–0.720	0.672	0.911	0.836

employee. In this evaluation cycle we have allowed and encouraged the participants to take the perspectives of both patients and healthcare professionals. This gives the participants an impression which data the employees can access.

The survey was answered from the perspective of a patient, since (almost) everybody can understand the requirements of a PHR as a patient. Furthermore, the views of healthcare professionals were already taken into account in the first cycles. A total of 92 respondents were recruited for the survey. To achieve the highest possible data quality, 28 data sets were excluded for various reasons (e.g. incomplete questionnaires), resulting in 64 data sets being included in the analysis. In general, the number of participants here is relatively low; however, since the survey represents only a part of the evaluation, the number of participants is sufficient and provides initial findings for the acceptance of blockchain-secured PHRs. Of the 64 participants, 42 (65.6%) were male and 22 (34.4%) were female. The age of the participants was between 18 and 49 years (average age: approximately 25.56 years).

Prior to the evaluation, we conducted various analyses[6] to ensure the validity and reliability of the collected data. Therefore, various quality measures were calculated and interpreted based on Weiber and Mühlhaus (2014). In a first step, Cronbach's alpha (CA) was calculated (see Table 3). Cronbach's Alpha measures the internal consistency of a scale and can range from − 1 to 1 (Cronbach 1947; Cronbach and Meehl 1955). The closer Cronbach's alpha approaches 1, the better a set of items explains a single unidimensional latent construct (Peter 1979; Nunnally and Bernstein 1994). For all constructs, the threshold value of 0.7 was exceeded and can therefore be considered as reliable (Weiber and Mühlhaus 2014). Furthermore, the corrected inter-scale correlation (CISC) and the inter-item correlation (IIC) were examined to check the constructs for internal consistency. IIC is another measure to evaluate reliability at the overall construct level. It represents the average correlation of all items assigned to a construct an can range from − 1 to 1 (Revelle 1979; Weiber and Mühlhaus 2014). The corrected inter-scale correlation can also range from − 1 to 1 and indicates how strongly an item correlates with the other items of a construct. Thereby it can be measured how distinctly the items differ from each other (Nunnally and Bernstein 1994; Weiber and Mühlhaus 2014). Again, the respective threshold values (CISC ≥ 0.5 and IIC ≥ 0.3) were met (Weiber and Mühlhaus 2014)

[6] The analyses were conducted with SPSS (version 26) and SmartPLS (version 3.2.9).

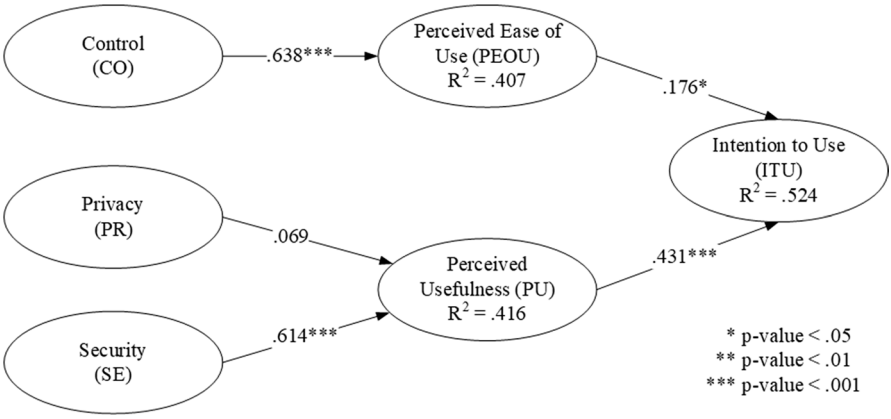

Fig. 7 PLS-SEM model

Therefore, the internal consistency of the constructs can be evaluated as fulfilled. Composite reliability (CR) and average variances extracted (AVE) were also used as additional quality measures. The required thresholds were also exceeded for these indicators (CR ≥ 0.6 and AVE ≥ 0.5) (Fornell and Larcker 1981; Bagozzi and Yi 1988); therefore, the reliability of the measurement is assumed. Furthermore, we used the Fornell–Larcker criterion to measure the validity of discriminants. This requires that a latent construct average shares a higher variance with the respective indicators (items) than with the other constructs of the model under investigation (Fornell and Larcker 1981).[7] Overall the results show that our items and constructs are reliable and well-functioning and that further evaluation can be started (Fig. 7).

After testing the reliability and validity, we investigated the relationship of the dependent variables. This was carried out using partial least squares structural equation modeling (PLS-SEM) (Hair et al. 2012, 2014). The analysis of the model confirms strong statistical correlations between CO and PEOU as well as between SE and PU and between PU and ITU. In addition, a (statistically) weaker correlation between PEOU and ITU was identified. The relatively low path correlation and the statistically insignificant correlation between PR and PU are also noteworthy. When interpreting the PLS-SEM model, interesting correlations can be identified. For example, the influence of SE (compared to PR) on PU is significantly higher. The participants consequently see the benefit more in in the high security of a blockchain-secured PHR and less in better privacy. This is also understandable in terms of argumentation, since the data are still stored online, as one user pointed out in the survey. Nevertheless, the detailed access management and tracking offers advantages for users. Furthermore, it must be noted that although the prototype we developed offers suitable usability (see PU and the PU–ITU relationship), PU has a significantly greater influence on ITU than PEOU. This is understandable in terms of argumentation for two main reasons. First, the application developed is still a

[7] The Fornell–Larcker criterion can be accessed here: https://bit.ly/37ML3ZM.

prototype that can be improved. Second, it makes sense that with a PHR *perceived usefulness* is in the foreground. For example, one user noted that function and security are priorities for him, while "the design is rather secondary." Furthermore, the average ratings for all constructs also indicate clearly positive evaluations (on average approximately 1.45 on a scale of − 3/3). When analyzing the average values, it can also be seen that the PU of the blockchain-secured EHR in particular was positively highlighted. Furthermore, the participants were asked to use free text fields to point out the strengths and improvement potential of the prototype. In particular, an improvement in accessibility (e.g. for people with visual impairments) and an emergency data set were suggested.

After each evaluation cycle, we gathered potential improvements from the received feedback; a summary is presented in Table 4. The next step of the evaluation should be in a field test. However, some adjustments are still required to perform this. To reach as many users as possible, additional interfaces to existing systems (e.g. hospital information systems) should be provided. This would enable the different actors in the health sector, in the long term, to achieve high or rapid adoption. In this context, analysis possibilities of the available data in terms of data analytics should also be discussed. For example, users could voluntarily and anonymously provide their data to the community (e.g. to research institutions) or offer them in the private (health) sector. Especially in this context, user attitudes regarding acceptance and privacy must be continuously recorded and analyzed, as our survey did not cover everyday use.

Table 4 Feedback from evaluation cycles

Evaluation cycles				Feedback
I	II	III	IV	
■				Add the option to delete documents
■				Add the medical specification (e.g. dentist) of the healthcare professionals
■				Improve the search function within the uploaded documents
■				List and highlight stakeholders with withdrawn permission
■	■			Improve document management from the employees' perspective
■	■			Simplify layout to enable intuitive design
■	■			Improve the response time
	■			Arrange the doctors so that the recently added are in first position
	■			Add icons to the interface to create a more intuitive user experience
	■	■		Extend sorting options (e.g. by doctor's letter or operation report)
		■		Add a button and an explanation for saving the QR code
		■		Add an emergency contact to the overview page
		■	■	Improve loading speed for the mobile website
			■	A sorting function was added to the folders
			■	In addition to data collection, analysis tools should be offered in the medium term
			■	The color representation of the icons and the font were harmonized with each other
			■	In the future, the barrier-free accessibility of the application should be improved
			■	An emergency data set has been set up that can be called up if necessary

Table 5 Key findings for the identified design principles

DP	Key findings
DP1	The application allows users to save various file types A document approach enables interoperability without complex interfaces High data volumes can be managed with appropriate scaling Different documents can be made available for different stakeholders
DP2	Traceability of transactions increases trust and confidence Permanent availability through decentralization reduces users' fears of not being able to manage access to their health data The authorization and authentication concept keeps the risk of abuse low
DP3	Users receive the information they need at a glance, and more detailed information and treatment histories can be viewed Patients can determine who can view which data and check when data have been queried

7 Discussion and implications

So far, the promising benefits of PHRs have usually been outweighed by data security and privacy concerns (Hoerbst et al. 2010; Adelmeyer et al. 2019). Blockchain technology has recently been discussed in the literature as an instrument to overcome this barrier (Beinke et al. 2019). In contrast to existing prototypes such as MedRec, OmniPHR or FHIRChain, we systematically identified issues, derived MRs and consolidated them into three DPs. Our findings contribute to the design knowledge base and might be transferred to further technological solutions in healthcare or other industries. The key findings for each DP are summarized in Table 5.

The suggested improvements were implemented in our blockchain-secured PHR. It can be customized to individual demands and serves as a secure, document-based platform (e.g. cloud repository) to exchange health-related information between patients and healthcare professionals. However, the developed solution is still a prototype intended to demonstrate access management for personal health records via blockchain and evaluating users' trust in such a solution. Therefore, challenges regarding to GDPR might occur. So far, some personal data (e.g. name, birthday) is stored in the blockchain. The personal data would have to be stored encrypted in an off-chain database. In this context, it has to be noted that the encryption key is stored in the blockchain and could therefore be accessed by the peer operators. In a productive solution, this could be solved by using a key management server that can be requested by the user.

7.1 Implications for practice

The implications for practice primarily affect patients and healthcare professionals. Patients mainly benefit from OSHealthRec because of the warranty of the data security. The blockchain supports that only authorized persons may access their health data. Compared to the status quo, in which the healthcare system is often a black box for patients, the transparency and traceability of OSHealthRec constitutes a major

improvement. Patients are empowered to self-manage and self-determine their data, and they can easily track the course of treatment. This reduces mistakes and unnecessary double treatments. In order to avoid the problem that patients hold back important information because they feel ashamed or they cannot assess the relevance, a healthcare professional can see all health information about a patient by default once he is authorized to access the data. However, if a patient wants an unbiased second opinion about a diagnosis he or she should be able to block specific files or information for a specific healthcare professional. This additional function could be implemented in a further development of our prototype. In cases of fraud or medical mistakes, every step is unchangeably tracked in the blockchain. Another benefit is the independence of central governmental organizations, as we recommend the formation of a consortium to operate the private blockchain. This consortium could, for example, be made up of associations of physicians, pharmacies and health insurance companies.

However, the self-administration of a PHR requires the motivation and effort of patients to learn the correct use and to continuously manage their personal account. Many patients, especially elderly people, might be deterred because they fear doing something wrong. Therefore, healthcare providers must encourage patients to use the PHR. Another potential problem is that trust in the blockchain technology requires an understanding of how it works. Therefore, given its novelty and complexity, healthcare professionals must explain and promote the technology to their patients.

Similar to the patients, the implementation of a blockchain-secured PHR would have implications for healthcare professionals as it affects their everyday work. First, a blockchain-secured PHR would increase cooperation with other healthcare providers. This requires clear communication and standardized files. The transfer of patient data and respective documents would also be easy without sending a fax or e-mail, which requires the correct address of the recipient. Second, improving the efficiency of administrative tasks allows doctors to spend more time with their patients. In addition, the tracking of every transaction makes it possible to reproduce treatment history and to detect mistakes or misuse. At the same time, this transparency reduces liability risks in case of unauthorized access. Furthermore, from the medical research perspective, healthcare professionals may use anonymized data from PHRs to investigate new diseases and therapies.

7.2 Implications for research

Apart from the implications for patients and healthcare professionals, determining the operator or operators of a blockchain remains necessary so that a blockchain-secured PHR can be implemented. It is essential that users trust the operators, since they are the only ones who can influence the transactions (Beck et al. 2018). Therefore, the question arises as to which actors (e.g. government, health insurance companies) are explicitly involved in the operation of the blockchain-secured EHR. Our proposal is that the operation should be run by a consortium of all relevant stakeholders (government, health insurance companies, associations, doctors etc.). The research task here is to weigh up competing interests and make a decision that puts the well-being of the patient first.

As development in the field of blockchain technology is rapidly advancing, it should be mentioned that the used Hyperledger Composer was deprecated in August 2019 and is therefore no longer being actively developed. It has been replaced by Hyperledger Fabric v1.4, which offers improvements in the programming model and further enhancements. In the meantime, Hyperledger Fabric has reached version 2.1, which shows the fast development of the technology. We are currently working on transferring our prototype to the current Hyperledger version to ensure permanent access to it. The functional enhancements of Hyperledger Fabric already provide better performance. Furthermore, since the main intention of our prototype is to generate design knowledge and determine its acceptance by users in the healthcare system, many options exist for further development. For example, the security of the solution can be improved, while the documents are available only encrypted on the document server and the key is stored in the document asset in the blockchain, thereby ensuring that only authorized users can decrypt the document. In addition, the application should be opened for further interest groups and, if necessary, made available to other institutions such as health insurance companies. In this way, the application would support even more use cases and experience broader acceptance. Finally, by preparing and integrating medical reports, the findings can be structured more clearly, and better correlations between the reports can be identified.

Overall, we conclude that blockchain technology constitutes a suitable solution for privacy concerns with regard to health-related data. A document-based online system requires no investments in hardware or software, and it can easily be accessed from any device with a web browser. Our findings make a contribution to the discipline of information systems. By applying DSR for the development of the PHR, design knowledge is generated and evaluated. It enhances the existing knowledge base and can be used by other researchers. According to Gregor and Hevner (2013) the developed artifact and corresponding DPs of type "Level 2: Nascent Design Theory" and mainly contribute to the prescriptive knowledge that describes how artifacts are designed. With the results of the final evaluation, we also contribute to descriptive knowledge by analyzing the effects of the implementation of the system.

8 Conclusion

While the advantages of PHRs are indisputable, their adoption is still hampered by data security and privacy concerns. Blockchain technology constitutes a promising solution to increase the trust in and safety of PHRs. Within a 1-year DSR project, we developed a blockchain-secured PHR. First, we identified nine domain-specific issues that were necessary to consider within the development phase. In the next step, we derived eight MRs that were consolidated in three DPs for blockchain-secured PHRs. After developing a prototype on the basis of Hyperledger Fabric, we conducted four evaluation cycles and continuously incorporated the feedback into the system. Our evaluation cycles do not represent a sufficient sample size for an international rollout. Quantitative field studies are required to investigate trust in and acceptance of blockchain technology within health-related use cases. Given the novelty and complexity, many patients are reluctant to trust an unknown security

mechanism. However, we conclude that blockchain technology offers promising potential to substantially improve healthcare. In future investigations the cooperation between the various stakeholder groups, such as pharmacies, hospitals, laboratories, and care services on a blockchain-secured system should be addressed.

Funding Open Access funding provided by Projekt DEAL. The authors would like to thank the experiment participants, the project team Timo Kopmann, Shafig Hussein Saleh, Linshan Shi, Feipeng Xu, for their valuable and substantive help, as well as the reviewers for their constructive feedback. This contribution was prepared within the research projects "Dorfgemeinschaft 2.0" (German Federal Ministry for Education and Research, funding code 16SV7453) and "Apotheke 2.0" (German Federal Ministry of Food and Agriculture, „Land.Digital", PT BLE).

Appendix

See Table 6.

Table 6 Constructs and item sources

Construct	Adapted definition	References
SE	The perception of the user regarding the PHR to protect the data, which includes, for instance, unauthorized modification, access or interference	Flavián and Guinalíu (2006) and Adelmeyer et al. (2019)
PR	Privacy describes the extent to which the user retains control over his or her own data. This includes basic concerns and compliance with (privacy) laws and no unauthorized disclosure of information	Flavián and Guinalíu (2006) and McLeod et al. (2009)
CO	CO is defined as the perceived control of the users when using the system. In the context of EHR, this includes in particular the ability to control the process of storing, retrieving and releasing data	Lee and Benbasat (2011) and Adelmeyer et al. (2019)
PEOU	PEOU defines how much effort is required for users to learn how to use the system. Since PHR gives the user control over his or her own data, the effort for the user should be relatively low, since possible operational errors can have a major impact	Davis (1989)
PU	Perceived usefulness describes the extent to which the use of block-chain-based PHR improves the availability and use of health data	Davis (1989)
ITU	The intention to voluntarily use the blockchain-secured PHR	Ermakova et al. (2014)

References

Adelmeyer M, Meier P, Teuteberg F (2019) Security and privacy of personal health records in cloud computing environments—an experimental exploration of the impact of storage solutions and data breaches. In: Wirtschaftsinformatik

Al-Aswad AM, Brownsell S, Palmer R, Nichol JP (2013) A review paper of the current status of electronic health records adoption worldwide: the gap between developed and developing countries. J Health Inform Dev Ctries 7(2):153–164

Amelung V, Bertram N, Binder S, Chase DP, Urbanski D (2016) Die elektronische Patientenakte. Fundament Einer Effektiven Und Effizienten Gesundheitsversorgung. Stiftung Münch (Hrsg.), Medhochzwei

Angst CM, Agarwal R, Downing J (2006) An empirical examination of the importance of defining the PHR for research and for practice. Robert H. Smith School Research Paper No. RHS-06–011.

Bagozzi RP, Yi Y (1988) On the evaluation of structural equation models. J Acad Mark Sci 16(1):74–94

Beck R, Czepluch JS, Lollike N, Malone S (2016) Blockchain – The gateway to trust-free cryptographic transactions. In: Paper presented at the twenty-fourth European conference on information systems (ECIS), Istanbul, 2016

Beck R, Avital M, Rossi M, Thatcher JB (2017) Blockchain technology in business and information systems research. Springer, Berlin

Beck R, Müller-Bloch C, King JL (2018) Governance in the blockchain economy: a framework and research agenda. J Assoc Inf Syst 19(10):1

Beinke JH, Nguyen D, Teuteberg F (2018) Towards a business model taxonomy of startups in the finance sector using blockchain. In: Paper presented at the thirty ninth international conference on information systems (ICIS), San Francisco, 2018

Beinke JH, Fitte C, Teuteberg F (2019) Towards a stakeholder-oriented blockchain-based architecture for electronic health records. J Med Internet Res 21:e13585

Burrington-Brown J, Fishel J, Fox L, Friedman B, Giannangelo K, Jacobs E, Lang D, Lemery C, Malchetske B, Morgan J, Murphy K (2005) Defining the personal health record. AHIMA releases definition, attributes of consumer health record. J AHIMA 76(6):24

Busse R, Geissler A, Aaviksoo A, Cots F, Häkkinen U, Kobel C, Mateus C, Or Z, O'Reilly J, Serdén L, Street A (2013) Diagnosis related groups in Europe: moving towards transparency, efficiency, and quality in hospitals? BMJ 346:f3197

Chao WC, Hu H, Ung COL, Cai Y (2013) Benefits and challenges of electronic health record system on stakeholders: a qualitative study of outpatient physicians. J Med Syst 37(4):9960

da Conceicao AF, da Silva FS, Rocha V, Locoro A, Barguil JM (2018) Eletronic health records using blockchain technology. Eletronic Health Records using Blockchain Technology. https://arxiv.org/pdf/1804.10078

Cronbach LJ (1947) Test "reliability": its meaning and determination. Psychometrika 12(1):1–16

Cronbach LJ, Meehl PE (1955) Construct validity in psychological tests. Psychol Bull 52(4):281

Dagher GG, Mohler J, Milojkovic M, Babu P (2018) Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 39:283–297

Davis FD (1986) A technology acceptance model for empirically testing new end-user information systems: theory and results. Massachusetts Institute of Technology, Cambridge

Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q Manag Inf Syst 13(3):319–339

Dey AK, Abowd GD, Salber D (2001) A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. Hum Comput Interact 16(2–4):97–166

Dugas M, Neuhaus P, Meidt A, Doods J, Storck M, Bruland P, Varghese J (2016) Portal of medical data models: information infrastructure for medical research and healthcare. Database 2016:bav121

e Estonia (2020) KSI Blockchain. https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/. Accessed 15 Aug 2020

Einaste T (2018) Blockchain and healthcare: the Estonian experience—e-Estonia. https://e-estonia.com/blockchain-healthcare-estonian-experience/. Accessed 15 Aug 2020

Ekblaw A, Azaria A, Halamka JD, Lippman A (2016) A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In: Proceedings of IEEE open & big data conference, vol 13

Ermakova T, Fabian B, Zarnekow R (2014) Acceptance of health clouds—a privacy calculus perspective. In: Proceedings of the European conference on information systems (ECIS) 2014, Tel Aviv, Israel, 9–11 June 2014
Esposito C, De Santis A, Tortora G, Chang H, Choo K-KR (2018) Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 5(1):31–37
Feldman SS, Buchalter S, Hayes LW (2018) Health information technology in healthcare quality and patient safety: literature review. JMIR Med Inform 6(2):e10264
Finck M (2018) Blockchains and the general data protection regulation. Blockchain regulation and governance in Europe. Cambridge University Press, Cambridge
Flavián C, Guinalíu M (2006) Consumer trust, perceived security and privacy Policy: three basic elements of loyalty to a website. Ind Manag Data Syst 106:601–620
Fornell C, Larcker DF (1981) Structural equation models with unobservable variables and measurement error: algebra and statistics. SAGE Publications, Los Angeles
Foronda C, MacWilliams B, McArthur E (2016) Interprofessional communication in healthcare: an integrative review. Nurse Educ Pract 19:36–40
Friedlmaier M, Tumasjan A, Welpe IM (2018) Disrupting industries with blockchain: the industry, venture capital funding, and regional distribution of blockchain ventures. In: Venture capital funding, and regional distribution of blockchain ventures (September 22, 2017). Proceedings of the 51st annual Hawaii international conference on system sciences (HICSS)
Gay V, Leijdekkers P (2015) Bringing health and fitness data together for connected health care: mobile apps as enablers of interoperability. J Med Internet Res 17(11):e260
Gillum J, Kao J, Larson J (2019) Millions of Americans' medical images and data are available on the internet. Anyone Can Take a Peek.—ProPublica. https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet. Accessed 15 Aug 2020
Gordon WJ, Catalini C (2018) Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J 16:224–230
Gregor S, Hevner AR (2013) Positioning and presenting design science research for maximum impact. MIS Q 37(2):337–355
Gregor S, Jones D (2007) The anatomy of a design theory. J Assoc Inf Syst 8(5):312–335
Gregor S, Kruse LC, Seidel S (2020) The anatomy of a design principle. J Assoc Inf Syst (forthcoming)
Guardtime (2020) Enterprise Blockchain. https://guardtime.com/. Accessed 14 Feb 2020
Haas P (Berteslmann S 2017). Elektronische Patientenakten. Dortmund
Hair JF, Sarstedt M, Ringle CM, Mena JA (2012) An assessment of the use of partial least squares structural equation modeling in marketing research. J Acad Mark Sci 40(3):414–433
Hair JF Jr, Sarstedt M, Hopkins L, Kuppelwieser VG (2014) Partial least squares structural equation modeling (PLS-SEM): an emerging tool in business research. Eur Bus Rev 26:106–121. https://doi.org/10.1108/EBR-10-2013-0128
Healthcare-IT-News (2018) The biggest healthcare data breaches of 2018 (so far). https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far. Accessed 15 Aug 2020
Heart T, Ben-Assuli O, Shabtai I (2017) A review of PHR, EMR and EHR integration: a more personalized healthcare and public health policy. Health Policy Technol 6(1):20–25
Hevner A, March ST, Park J, Ram S (2004) Design science in information systems research. MIS Q 28:75–105
Hoerbst A, Kohl CD, Knaup P, Ammenwerth E (2010) Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens. Int J Med Inform 79(2):81–89
Holmström J, Ketokivi M, Hameri A (2009) Bridging practice and theory: a design science approach. Decis Sci 40(1):65–87
Kerkmann C, Micijevic A (2019) Millionen Patientendaten ungeschützt im Netz aufgetaucht. https://www.handelsblatt.com/technik/sicherheit-im-netz/ungesicherte-server-millionen-patientendaten-ungeschuetzt-im-netz-aufgetaucht/25023120.html?ticket=ST-8765679-dAJDHEDbbnOlS6UhubS5-ap6. Accessed 15 Aug 2020
Klecun E (2016) Transforming healthcare: policy discourses of IT and patient-centred care. Eur J Inf Syst 25(1):64–76
Kumar NM, Mallick PK (2018) Blockchain technology for security issues and challenges in IoT. Procedia Comput Sci 132:1815–1823
Kuo T-T, Kim H-E, Ohno-Machado L (2017) Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 24(6):1211–1220

Lee YE, Benbasat I (2011) Research note—the influence of trade-off difficulty caused by preference elicitation methods on user acceptance of recommendation agents across loss and gain conditions. Inf Syst Res 22(4):867–884
Leeming G, Cunningham J, Ainsworth J (2019) A ledger of me: personalizing healthcare using blockchain technology. Front Med 6:1–10
Linn LA, Koo MB (2016) Blockchain for health data and its potential use in health it and health care related research. In: ONC/NIST use of blockchain for healthcare and research workshop. ONC/NIST, Gaithersburg, Maryland, United States
Lune H, Berg BL (2017) Qualitative research methods for the social sciences (9th, Global edn). Essex. Pearson Education Ltd
McLeod A, Pippin S, Catania V (2009) Using technology acceptance theory to model individual differences in tax software use. In: AMCIS 2009 proceedings, p 811
Meier P, Beinke JH, Fitte C, Behne A, Teuteberg F (2019) FeelFit—design and evaluation of a conversational agent to enhance health awareness. In: Proceedings international conference on information systems (ICIS 2019), Munich
Mettler M (2016) Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th international conference on e-Health networking, applications and services (Healthcom). IEEE, pp 1–3
Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system
Nohl-Deryk P, Brinkmann JK, Gerlach FM, Schreyögg J, Achelrod D (2018) Barriers to digitalisation of healthcare in Germany: a survey of experts. Gesundheitswesen (Bundesverband Der Arzte Des Offentlichen Gesundheitsdienstes (Germany)) 80(11):939–945
Nunnally JC, Bernstein IH (1994) Psychometric theory 3E. Tata McGraw-Hill Education, New York
O'Donoghue O, Vazirani AA, Brindley D, Meinert E (2019) Design choices and trade-offs in health care blockchain implementations: systematic review. J Med Internet Res 21(5):e12426
Oemig F, Blobel B (2014) Natural language processing supporting interoperability in healthcare. In: Biemann C, Mehler A (eds) Text mining. Springer, Cham, pp 137–156
Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manage Inf Syst 24(3):45–77
Peter JP (1979) Reliability: a review of psychometric basics and recent marketing practices. J Mark Res 16(1):6–17
Plattner H, Meinel C, Weinberg U (2009) Design thinking. Springer, Berlin
Poston RS, Reynolds RB, Gillenson ML (2006) Technology solutions for improving accuracy and availability of healthcare records. Inf Syst Manag 24(1):59–71
Revelle W (1979) Hierarchical cluster analysis and the internal structure of tests. Multivar Behav Res 14(1):57–74
Risius M, Spohrer K (2017) A blockchain research framework. Bus Inf Syst Eng 59(6):385–409
Roehrs A, da Costa CA, da Rosa Righi R (2017) OmniPHR: a distributed architecture model to integrate personal health records. J Biomed Inform 71:70–81
Rono DK (2016) A restful e-health interoperability platform: case of Nairobi County health facilities. Strathmore University, Nairobi
Rückeshäuser N (2017) Do we really want blockchain-based accounting? Decentralized consensus as enabler of management override of internal controls. In: Leimeister JM, Brenner W (Hrsg.) Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, pp 16–30
Seitz J, Wickramasinghe N (2017) Blockchain technology in e-health: The case of electronic prescriptions in Germany. In: XVII international scientific conference on industrial systems.
Sousa J, Bessani A, Vukolic M (2018) A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In: 2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN). IEEE, pp 51–58
Stagnaro C (2017) White paper: innovative blockchain uses in health care. Freed Associates, Kensington
Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media Inc, Newton
Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ (2006) Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc 13(2):121–126
Tavares J, Oliveira T (2016) Electronic health record patient portal adoption by health care consumers: an acceptance model and survey. J Med Internet Res 18(3):e49
Venable J, Pries-Heje J, Baskerville R (2016) FEDS: a framework for evaluation in design science research. Eur J Inf Syst 25(1):77–89

Veseli H, Kopanitsa G, Demski H (2012) Standardized EHR interoperability: preliminary results of a German pilot project using the archetype methodology. Stud Health Technol Inform 180(180):646–650
vom Brocke J, Simons A, Niehaves B, Riemer K, Plattfaut R, Cleven A, Reimer K (2009) Reconstructing the giant: on the importance of rigour in documenting the literature search process. In: 17th European conference on information systems, vol 9, pp 2206–2217
Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J (2016) Untrusted business process monitoring and execution using blockchain. In: International conference on business process management. Springer, pp 329–347
Webster J, Watson RT (2002) Analyzing the past to prepare for the future: writing a literature review. MIS Q 26(2):xiii–xxiii
Weiber R, Mühlhaus D (2014) Strukturgleichungsmodellierung: Eine anwendungsorientierte Einführung in die Kausalanalyse mit Hilfe von AMOS, SmartPLS und SPSS. Springer, Berlin
White A, Danis M (2013) Enhancing patient-centered communication and collaboration by using the electronic health record in the examination room. JAMA 309(22):2327–2328
Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST (2018) FHIRChain: applying blockchain to securely and scalably share clinical data. Computa Struct Biotechnol J 16:267–278