Using Blockchain in PHR (Personal Health Record) Systems

Ryan Raffoul

Supervisor: Dr. Samet

COMP-4990 University of Windsor

Abstract

In this Literature Review, summarized will be articles on three topics, Personal Health Records, Blockchain, and Blockchain in Personal Health Records. Advantages, disadvantages, and a comparison will be given at the end of each topic.

A Personal Health Record (PHR) is a health record where health data and other information related to the care of a patient is maintained by the patient. The four articles discussed below deal with the benefits of a PHR, characteristics of an ideal PHR, assessment of a PHR, and the security of PHRs. The agreed upon conclusion is that if the PHRs main constraints can be limited, the overall potential is endless.

A Blockchain is a system in which a record of transactions made in any industry are maintained across several computers that are linked in a peer-to-peer network. The four articles discussed below on Blockchain are an overview of the architecture of a Blockchain, functionalities and implications of a Blockchain, a code implementation of a simple Blockchain, and a critical analysis of Blockchain technology. The agreed upon conclusion is that a Blockchain can be very beneficial and secure in all industries but has serious scalability issues.

Using Blockchain in a PHR system involves storing a patient’s healthcare data on a Blockchain and allowing the patient to easily and securely view and control who can see their data. The four articles discussed below on using Blockchain in a PHR system includes a systematic review, a data sharing model, feasibility, and performance.

The conclusion of this Literature Review is that a PHR based Blockchain has great potential to easily view and manage personal medical data while considering security and privacy concerns.

Review of Literature

Personal Health Records (PHRs)

In *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, a personal health record is defined as "an electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment" (Tang et al., 2006). There has been a remarkable upsurge in the adoption of PHR systems for patients and consumers as PHRs have become much more than just a simple static repository for a patient's data. PHRs can combine data, knowledge, and software tools to help patients become active participants in their own healthcare. When a PHR is integrated with a EHR (Electronic Health Record, an electronic version of a patient's medical history, that is maintained by the provider over time), this provides greater benefits than a stand-alone system for consumers. Tang et al. 2006 states that the main goal of PHRs is to "include tools to help individuals take a more active role in their own health. In part, PHRs represent a repository for patient data, but PHR systems can also include decision-support capabilities that can assist patients in managing chronic conditions." A PHR includes health information that the individual creates or accepts and manages. This is different from a paper chart that a physician might have for a patient although a future goal of PHRs is an environment in which health information about an individual can flow seamlessly among systems used by authorized health professionals, caregivers, and the patient, when the patient authorizes such sharing. A few approaches to create and manage PHRs are discussed. The main approach is a patient can create their PHR record using some sort of application and then control the sharing of this data. Another approach is a EHR created by a physician combined with any additional data entered by the patient. The last approach is a PHR where patients can view all their data recorded by a medical provider's EHR. Some common data sources involved with a PHR will include a problem list, procedures, major illnesses, allergy data, etc. The main benefits of a PHR for patients is greater patient access to a wider array of credible health information, data, and knowledge. The main payment for a PHR is still undecided although some combination of a patient and health-care provider is advised. The technological architecture must provide interoperability, support the same communications, messaging, and content encoding standards as other health information systems. This includes advanced security measures and authentication as a patient's sensitive data is at stake. The main barrier to the adoption and creation of PHRs is both privacy and security concerns. All levels of government are beginning to embrace PHRs, and this should continue and expand in the future.

In *What it Takes: Characteristics of the Ideal Personal Health Record*, the wider adoption of PHRs, the computer competency, internet access, and health literacy are discussed. A personal health record is defined as a "tool to use in sharing health information, increasing health understanding, and helping transform patients into better educated consumers of health care" (Kahn et al., 2009). A disconnect between PHRs and user requirements is discussed as the information a user wants from the PHR is not always considered. This article states the main agent to deliver a PHR is a mobile device with some type of large security and authentication measures. The main challenges of a PHR according to this article is cost concerns of implementation, information privacy concerns, design concerns, technical barriers, policy barriers, and the inability to share information across organizations. It is stated that "when the barriers to PHRs are solved, a PHR will be become invaluable to both patients and health-care providers" (Kahn et al., 2009). Constant internet access and improved computer competency is very important to get correct information for a PHR from a user, this is especially important for elderly patients. Better health literacy for patients and health-care providers may also be required. Some approaches to PHRs that can be implemented are one large PHR to go across all patient data or a specialized PHR, each for a different function. PHRs can be developed worldwide and even go across countries in the future. There is a case for optimism that this topic is only reaching its beginning stages and will continue to grow in the future.

In *Value of Personal Health Record (PHR) Systems*, a full assessment of the potential value of PHR systems, looking at both the costs and benefits is given. “We examine provider-tethered, payer-tethered, and third-party PHRs, as well as idealized interoperable PHRs. An analytical model was developed that considered eight PHR application and infrastructure functions” (Kaelber et al., 2008). The article states that PHR analysis shows that all forms and implementations have initial net negative value but will show their true value over time. “Interoperable PHRs provide the most value, followed by third-party PHRs and payer-tethered PHRs also showing positive net value. Provider-tethered PHRs constantly demonstrating negative net value” (Kaelber et al., 2008). The four-step method given in this article to determine the true value of PHRs is technology and data collection, evidence framework, evidence synthesis, and a model development. A list of functions sorted by application and infrastructure functions is given. Application functions include medication renewals, e-visits, and pre-encounter questionnaires. Infrastructure functions include sharing test results and sharing a list of medications. The result of these methods is an annual benefit of PHR functions would create a huge benefit when used over time. Keys to achieving this value include developing and adopting of standards electronic data exchange among PHRs, design of business models that align who is paying for and receiving the benefits from these systems, and deployment strategies that maximize the number of users per PHR installation.

In *Personal Health Record Systems and Their Security Protection*, a complete analysis of the security protection of personal health record systems is given. Different PHR systems are investigated based on their security functions and security issues. The focus of healthcare has shifted from the healthcare providers approach to a more consumer-oriented approach. Allowing patients to access their own records will encourage patients to be involved in their own healthcare and that will strengthen the patient–provider relationship and will enhance the effective healthcare management. The authors states that current security mechanisms are not adequate, and they have proposed some security mechanisms to tackle these problems. Some security issues discussed in this article are masquerading, unauthorized use of resources, unauthorized disclosure and flow of information, unauthorized alteration of resources and information, repudiation of actions, and unauthorized denial of service. The article discusses the importance and significance of a web based PHR system and how this can “impact healthcare serving as a single source of health information that is accessible from anywhere in the world and people’s health information could be under the shared control of the individual and their healthcare provider” (Win et al., 2006). A outside of the box alternative given by the authors is a health kiosk that could serve as a sort of healthcare ATM-style interface. This includes ways for users to manage, view, and update all their medical data. A patient’s access to their healthcare information is seen as both a positive and negative given that the two most important aspects of a PHR are accuracy and security. A highly advanced encryption method must be used to protect the integrity of the data. Some security measures discussed are stronger authentication (possibly face ID), better confidentiality, and specialized availability. The challenges presented to these security measures are this does not give 100% security and there be some web-based application vulnerabilities.

Based on these four articles on different topics within Personal Health Records all agree that the potential of PHRs is endless and we are only beginning to understand and implement this technology. Some advantages agreed upon are that patients can take an active role in their own healthcare, patients can be organized with healthcare data, health data can be accessed and tracked continuously, and a patient can have a better understanding of their own care and treatment for short-term and long-term illnesses. Some disadvantages agreed upon are authentication security, privacy concerns, health literacy, and data integrity. Some topics within PHRs that are not agreed upon is allowing a user to enter their data without the use of a EHR to verify, who is trusted to view and alter a patient's PHR, how to implement the PHR with different approaches, and who would be the main stakeholders.

Blockchain

In *Blockchain Technology Overview*, a high-level overview of Blockchain technology is given to understand how Blockchain technology works. A Blockchain is defined in this article as "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)" (Yaga et al., 2018). Blockchains are decentralized, secure, immutable, and chronological. A Blockchain enables a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network, no transaction can be changed once published. Blockchains are made up of blocks that contain any type of data, a hash of the current block, and a copy of the previous block's hash. There are two kinds of Blockchains, permission and permission-less. In a permission Blockchain, users publishing blocks must be authorized by some authority that is centralized or decentralized. In a permission-less Blockchain, users can publish blocks without any authority checking and accepting the block. A Blockchain follows a distributed consensus model where a new block can only be added if a consensus is reached by the other blocks. This is achieved by using a decentralized ledger where each user gets a copy of the Blockchain. A Blockchain is usually implemented using a peer-to-peer network and not a normal server-client network. Cryptographic hash functions are used to create the new blocks and ensure data integrity. This is achieved by giving each block a hash function and a copy of the previous block's hash. Then, if data is changed, the block's hash will change then make all subsequent blocks invalid. Proof-of-work is a feature of Blockchain where a user can publish a new block by being the first to solve a problem. Some other consensus models discussed are proof of authority, proof of identity, proof of elapsed time, and round robin. Forks are another feature used in a Blockchain, these are changes to a Blockchain's network and data structures. The two types of forks discussed in Blockchain are soft and hard. A main feature of a Blockchain is smart contracts. Smart contracts are programs and data contained on the Blockchain to perform actions when a specific condition is met. Some limitations of Blockchain are the immutability of data, users involved in the Blockchain's governance, cybersecurity, malicious attacks, resource utilization, and hash function infrastructure. The applications of Blockchain are endless and can be integrated with almost every industry. "Blockchain technology is a new tool with potential applications for organizations, enabling secure transactions without the need for a central authority" (Yang et al., 2018).

In *Blockchain – A Disruptive Technology*, functionalities of Blockchains, implications of Blockchains, smart contracts, and future trends are discussed. The article states "Blockchain technology and distributed ledgers are attracting massive attention and have triggered and will continue to trigger multiple projects in different industries" (Nofer et al., 2017). The main functionalities of Blockchain discussed are the creation of blocks, the cryptographic hash functions used to validate blocks and ensure integrity, a nonce used in which a random number is used to verify the hash, consensus algorithms used to validate and add blocks, and the distributed ledger system. The limitations of Blockchain discussed are malware attacks, performance problems, loss of data, communication failures, and scalability issues. Smart contracts are discussed briefly, defining smart contracts as a combination of "computer protocols with user interfaces to execute the terms of a contract" (Nofer et al., 2017). Application of Blockchain include crypto-currencies, insurance, notary public, healthcare, music, and internet applications. Some future trends of Blockchain discussed are that Blockchain could eventually change politics and our entire society.

In *What is the Blockchain,* a brief code implementation of a sample Blockchain is given. The article states that Blockchain is built on a matter of trust and the most important aspect of a Blockchain is establishing trust in a decentralized distributed system. Implementations of hash functions, verification, and a simple Blockchain are given. "A hash can be thought of as an encrypted version of the original string from which it is impossible to derive the original string" (Di Pierro et al., 2019). Examples of the hash implementations used are SHA1, SHA128, and SHA512. A sample hash function written in the programming language Python is given. A SHA1 algorithm is used to generate a hash and return to the Blockchain a timestamp, data, previous block's hash, and the hash that is created for the current block. A verification algorithm is given where blocks are looped through making sure that the current block's previous hash is equal to the previous block's hash. This is a central rule of Blockchain. The last algorithm given is a Blockchain class that can encapsulate everything and create and maintain the Blockchain. Future implementations could follow or build upon the implementation given.

In *Do you need a Blockchain,* a critical analysis is done to discover if Blockchain is indeed the appropriate technical solution for a particular application scenario. The 3 use cases discussed by the authors are supply chain management, international payments, and decentralized autonomous organizations. The article states that "Blockchain is being praised as a technological innovation which allows to revolutionize how society trades and interacts. This reputation is attributable to its properties of allowing mutually trusting entities to exchange financial value and interact without relying on a trusted third party. A blockchain moreover provides an integrity protected data storage and allows to provide process transparency" (Gervais et al., 2018). Permission and permission-less Blockchains are discussed, and which one may benefit who, for example a permission Blockchain is good for a Hyperledger while a permissionless Blockchain is good for Bitcoin. Some properties that all Blockchains must inherit according to the authors are public verifiability, transparency, privacy, integrity, redundancy, and a trust anchor. A flow diagram is given to show if a Blockchain really is needed for these industries. Some questions asked are do you need to store state, are all writers known, is data immutability important, and can public verifiably be implemented. The article concluded that a Blockchain can be used if your problem can be solved by the functionality Blockchain provides. Some future use cases discussed that can be solved by Blockchain are trading exchange, internet of things, healthcare, and e-voting.

Based on the four above articles relating to Blockchain, the main advantages of a Blockchain are its security due to its cryptographic hash functions and block rules, the data integrity based on the immutability of the data within the Blockchain, the decentralization of the Blockchain which will make it hard to hack as there is no central authority, and an individual control of data. The main disadvantages discussed are scalability issues within the Blockchain due to the redundancy of data, inefficiency of the Blockchain overall, immutable data that cannot be altered (also an advantage), and the integration with other applications or third-party services. Some topics within Blockchain that are not agreed upon are whether to implement a permission or permission-less Blockchain, which hash functions to use based on the data available, and how a Blockchain should be scaled.

Blockchain in Personal Health Records

In *Blockchain Personal Health Records: Systematic Review*, a deep-dive review into using a Blockchain for PHRs is done. This article examines the current landscape, design choices, limitations, and future directions of a Blockchain-based PHR. A Blockchain will enable more secure, transparent, and equitable data management, this is specifically important in the healthcare industry. A Blockchain based PHR will have the specific advantage of distributed data access, data control, and ownership by the end users. Some advantages of PHRs discussed are patient empowerment and reduced healthcare costs. Due to a Blockchain's decentralized nature, in which data is held by the end users, a PHR Blockchain would be very beneficial and important. The research state of Blockchain in PHRs is still in its infancy with much more theoretical foundations of a Blockchain based PHR being discussed and not much implementation. The main aspects of a Blockchain are discussed, including public and private Blockchains. Some other aspects discussed are decentralization, immutability, transparency, scalability, and smart contracts. All these aspects were discussed in detail in the Blockchain portion of this review. The main method for review used was data abstraction where a standardized data collection model was created using Microsoft Excel. Data elements were sorted into General, Blockchain, and PHR. Some data elements used in the Blockchain section are the type of Blockchain, the data storage used, and the solution to scalability. Some data elements for the PHR section used were the data owner, privacy standard, and read privileges. The main results of this study were that the main interest group in a Blockchain PHR are from a computer science background as opposed to a medical background, the maturity level of implementation of a Blockchain PHR is in its infancy but is still steadily growing over time with the implementation and research growing year by year, and at this stage concepts, models and frameworks are being implemented more than prototypes and applications. Current limitations of a Blockchain PHR discussed are scalability, privacy, and usability. One scalability issue of particular importance discussed is the ability of a Blockchain to store medical images which will cause slowness and retrieval delays. Future directions for study discussed include improving the user experience, integration with existing and new systems, and compliance with regulations and development of government processes. The principal finding of this study was that a Blockchain PHR system is actively growing but scalability is a real issue.

In *Blockchain Based Secret-Data Sharing Model for Personal Health Record System*, a secret-data sharing model for PHR systems using Blockchain is presented. This article states that the transparent property of Blockchain may cause privacy and confidentiality concerns when combined with a PHR and the overall large amount of healthcare data can overwhelm and overload Blockchain usages. “A blockchain based secret-data sharing model is proposed by using a proxy re-encryption technique to support the PHRs in this work. Some potential attacks which can attempt on the proposed model and how the model can handle such attempts is also discussed” (Thwin et al., 2018). An access control mechanism for a PHR presented contains three main components. These are identifying the user with a high-level mechanism, authenticating the user, and authorizing the user to only certain permissions and accesses. The Blockchain solution discussed includes storing the healthcare data in a distributed manner, on-demand access, and supporting a cryptographic approach. The privacy access of PHRs and Blockchain are the most important aspect of this model. The user who owns their PHR has the right to share their information with those who they consent to, usually doctors, nurses, and administrative staffs. The crypto key system will be the most important aspect of privacy and security. The challenges of implementing this are performance issues, scalability concerns, privacy, and energy consumption due to redundancy. Some related works that can be accessed are MediBloc, OmniPHR, and MedVault. The proposed secret data sharing model is built off these related works, focusing on storing encrypted data and accessing this encrypted data. The article concludes the main advantages of this secret model are its decentralized nature and its transparency while its main disadvantages are privacy and scalability.

In *Is Blockchain Technology Suitable for Managing Personal Health Records, Mixed-Methods Study to Test Feasibility*, a comprehensive study is done to examine if a Blockchain is feasible in managing PHR records. “The purpose of this study was to investigate the usefulness of blockchains in the medical field in relation to transactions with and propagation of PHRs in a private blockchain” (Park et al., 2019). “The ubiquity of mobile phones and rapid spread of wearable devices have greatly increased the amount and accuracy of data directly generated by patients outside of medical facilities” (Park et al., 2019). These types of data are the future and a PHR can make this much more personalized. Several studies have proposed the use of blockchain technology as a potential way to improve current PHR systems, which restrict access to recording and sharing of data. Advantages of using a Blockchain for a PHR system include its reliability, transparency, and security. The study design used for this article was done by constructing a private Blockchain using Ethereum, and verification was conducted using the PHR of 300 patients. The network consisted of one hospital node and 300 patient nodes. The data transaction, propagation, and reproducibility of the Blockchain PHR was studied. The overall result was that 24.7% of patient records were not loaded into the Blockchain due to the data block size of the transaction block. The remaining records were separated into groups and the transaction time was recorded.

In *Analyzing the Performance of a Blockchain-based Personal Health Record Implementation*, an implementation of a PHR that integrates distributed health records using Blockchain is analyzed. Health records are "commonly scattered in multiple places and are not integrated" (Roehrs et al., 2019) and therefore a PHR can come in handy where a user can view and have a clear view of all their medical data. The aim of this study was to implement and evaluate the "PHR model that integrates distributed health records using blockchain technology and the *open*EHR interoperability standard" (Roehrs et al., 2019). OmniPHR architecture was followed, which describes the infrastructure of an ideal PHR. The methods involved are implanting an unfinished prototype from different production databases and evaluating performance and integration of this. Some non-functional requirements, such as CPU usage and network usage are also recorded. The results were done studying a dataset of more than 40 thousand adult patients from two different hospital databases. The overall principal findings were that the Blockchain prototype implemented achieved 98% availability and the data distributed by the Blockchain can be recovered or retrieved with low latency.

Based on the four above articles relating to Blockchain in PHR, the main advantages agreed upon are secure access to a patient's data, transparent medical data due to its decentralized data access, full healthcare data ownership by patients, and overall greater patient empowerment. The main disadvantages of Blockchain in PHR agreed upon are scalability issues with a Blockchain overall but specifically with a PHR due to the large amount of medical data that is available, privacy concerns on who can see a patient's data, the overall useability of Blockchain with a PHR, and Government policies regarding healthcare access and permissions. Some Blockchain in PHR topics not agreed upon are the type of Blockchain to use, the type of data to store, the correct user interface, and how to solve the scalability issue with a Blockchain.

Conclusion

A Personal Health Record (PHR) has the ability for a patient to have all their data in one place which can be very useful to share and manage data. Blockchain can securely store and retrieve this medical data due to its immutability and decentralization. In conclusion, a PHR based Blockchain has great potential to easily view and manage personal medical data while considering security and privacy concerns.

References

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. Journal of the American Medical Informatics Association: JAMIA, 13(2), 121–126. https://doi.org/10.1197/jamia.M2025

Kahn, J. S., Aulakh, V., & Bosworth, A. (2009). What it takes: characteristics of the ideal personal health record. *Health affairs (Project Hope)*, *28*(2), 369–376. https://doi.org/10.1377/hlthaff.28.2.369

Kaelber, D., & Pan, E. C. (2008). The value of personal health record (PHR) systems. *AMIA ... Annual Symposium proceedings. AMIA Symposium*, *2008*, 343–347.

Win, Khin & Susilo, Willy & Mu, Yi. (2006). Personal Health Record Systems and Their Security Protection. Journal of medical systems. 30. 309-15. 10.1007/s10916-006-9019-y.

Yaga, D. , Mell, P. , Roby, N. and Scarfone, K. (2018), Blockchain Technology Overview, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8202

Nofer, M., Gomber, P., Hinz, O. *et al.* Blockchain. *Bus Inf Syst Eng* **59,** 183–187 (2017). https://doi.org/10.1007/s12599-017-0467-3

Di Pierro, Massimo. (2017). What Is the Blockchain?, Computing in Science & Engineering. 19. 92-95. 10.1109/MCSE.2017.3421554.

Di Pierro, Massimo. (2017). What Is the Blockchain?. Computing in Science & Engineering. 19. 92-95. 10.1109/MCSE.2017.3421554.

Fang HSA, Tan TH, Tan YFC, Tan CJM. (2021).
Blockchain Personal Health Records: Systematic Review
J Med Internet Res 2021;23(4): e25094

T. T. Thwin and S. Vasupongayya, "Blockchain Based Secret-Data Sharing Model for Personal Health Record System," *2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA)*, 2018, pp. 196-201, doi: 10.1109/ICAICTA.2018.8541296.

Park YR, Lee E, Na W, Park S, Lee Y, Lee J
Is Blockchain Technology Suitable for Managing Personal Health Records? Mixed-Methods Study to Test Feasibility
J Med Internet Res 2019;21(2):e12533

Roehrs, Alex & André da Costa, Cristiano & Righi, Rodrigo & Silva, Valter & Goldim, Jose & Schmidt, Douglas. (2019). Analyzing the Performance of a Blockchain-based Personal Health Record Implementation. Journal of Biomedical Informatics. 92. 103140. 10.1016/j.jbi.2019.103140.