HHS Public Access

Author manuscript

Blockchain Healthc Today. Author manuscript; available in PMC 2020 June 10.

Published in final edited form as:

Blockchain Healthc Today. 2019 ; 2: . doi:10.30953/bhty.v2.38.

DMMS: A Decentralized Blockchain Ledger for the Management of Medication Histories

Patrick Li[1], **Scott D. Nelson**[2], **Bradley A. Malin**[2,3,4], **You Chen**[2]

[1]Computer Science, Saratoga High School, Saratoga, CA, USA;

[2]Department of Biomedical Informatics, Vanderbilt University Medical Center, Nashville, TN, USA;

[3]Department of Biostatistics, School of Medicine, Vanderbilt University Medical Center, Nashville, TN, USA;

[4]Department of Electrical Engineering & Computer Science, School of Engineering, Vanderbilt University, Nashville, TN, USA

Abstract

Background: Access to accurate and complete medication histories across healthcare institutions enables effective patient care. Histories across healthcare institutions currently rely on centralized systems for sharing medication data. However, there is a lack of efficient mechanisms to ensure that medication histories transferred from one institution to another are accurate, secure, and trustworthy.

Methods: In this article, we introduce a decentralized medication management system (DMMS) that leverages the advantages of blockchain to manage medication histories. DMMS is realized as a decentralized network under the hyperledger fabric framework. Based on the network, we designed an architecture, within which each prescriber can create prescriptions for each patient and perform queries about historical prescriptions accordingly. finally, we analyzed the advantages of DMMS over centralized systems in terms of accuracy, security, trustworthiness, and privacy.

Results: We developed a proof of concept to showcase DMMS. In this system, a prescriber prescribes medications for a patient and then encrypts the prescriptions via the patient's public keys. Patients can query their own prescriptions from different histories across healthcare institutions and then decrypt the prescriptions via their private keys. At the same time, a prescriber can query a patient's prescription records across healthcare institutions after approval from the

Corresponding Author: You Chen, PhD, Department of Biomedical Informatics, Vanderbilt University Medical Center, 2525 West End Ave, Suite 1475, Nashville, TN 37203, USA. you.chen@vumc.org.

Contributors

Patrick Li performed literature review, decentralized ledger solution design, architecture design, proof of concept development, evaluation and interpretation of the proof of the concept, and writing of the manuscript. Scott D. Nelson performed literature review, architecture design, evaluation and interpretation of the proof of the concept, and revising of the manuscript. Bradley A. Malin performed literature review, architecture design, evaluation and interpretation of the proof of the concept, and revising of the manuscript. You Chen performed literature review, decentralized ledger solution design, architecture design, proof of concept development, evaluation and interpretation of the proof of the concept, and writing of the manuscript.

Conflicts of Interests

The authors declare no competing interests with respect to research, authorship and/or publication of this article.

patient. Analytic results show that DMMS can improve security, trustworthiness, and privacy in medication history sharing and exchanging across healthcare institutions. In addition, we discuss the potential for DMMS in e-prescribing markets.

Conclusions: This study shows that a distributed secure ledger can enable reliable, interoperable, and accurate medication history sharing.

Keywords

Blockchain Ledger; Decentralized; Hyperledger Fabric Framework; Medication Histories

It is important to provide prescribers with the most recent knowledge about the set of medications that a patient is taking, has taken in the past, and those he/she may be allergic to. Such knowledge influences the decision-making process during a patient encounter, as medications can interfere with laboratory tests, as well as informs which, if any, additional medications to prescribe. Yet, medication errors are common, which is unfortunate because incomplete medication lists increase the risk of medication errors and adverse drug effects (ADEs).[1] Notably, 3% of errors correspond to the omission of life-saving medications and 41% of errors have the potential to cause moderate to severe harm.[2] More than 770,000 injuries or deaths occur annually due to ADEs, which often arise as a result of errors in medication lists.[3–8] Moreover, when medication histories are incomplete at the time of patient admission, they can be the source of complications, including longer hospital stays.[9,10]

Electronic Health Records (EHRs) are composed of private, highly sensitive information, including medication records. However, the process of storing, transferring, and sharing data (e.g., historical prescriptions) across multiple entities is complicated and inconvenient. Large healthcare systems often rely on third-party systems (e.g., Epic, Cerner, and SureScripts) to handle the sharing and transfer of medication records. These systems rely on private centralized databases, which is problematic because they are susceptible to costly intrusions, such as ransomware attacks or data leaks. In 2016, the health records of 16.6 million Americans were leaked, a number that increased by 26% in 2017.[11] The main drawback of centralized systems is their reliance on a central server to perform all network functions, which allows for a single point of failure. The moment the central server is compromised, the entire network is suspended and becomes susceptible to alterations.

Beyond security risks, private centralized systems are also extraordinarily costly, often requiring hundreds of millions of dollars to install, integrate, and manage.[12] Even with the assistance of EHR vendors, medication lists are often outdated between encounters with the healthcare system, especially when a patient sees multiple care providers. Since most healthcare institutions (HI) maintain an internal copy of a patient's EHR, if a care provider from Hospital A makes changes to the patient's medication list, Hospital B is unlikely to be aware of these changes. The situation increases in complexity as patients work with an increasing number of care providers and pick up their prescriptions from different pharmacies. care providers usually obtain information about a patient's medication history through an initial interview,[13] but this can be unreliable due to human error and patients

being poor historians (i.e., not knowing the medications they take) or having low health literacy.

Given the deficiencies of the status quo, we believe that a cross-institution, private, immutable ledger of personal patient medication records has the potential to address the aforementioned issues, especially in an environment where no single person takes responsibility for maintaining an accurate medication list. This network can be realized with decentralized systems because a distributed ledger can solve roadblocks with medication record transfer and sharing. Moreover, the security protocols of a distributed ledger are more reliable than centralized systems. Thus, we propose a decentralized medication management system (DMMS), which leverages blockchain technology to improve security, trustworthiness, and privacy in the sharing and transfer of medication histories. We will be focusing on US histories across healthcare institutions. This article is organized into two primary sections. First, we depict the DMMS architecture and illustrate its advantages in terms of security, trustworthiness, and privacy. Second, we present a DMMS prototype, investigate its potential effect on e-prescriptions, and expand on the future implications of our framework.

DECENTRALIZED NETWORK

A decentralized network, also known as a peer-to-peer platform, is a distributed architecture that allocates its resources to a host of nodes, functioning together to make decisions on behalf of the network. In a decentralized system, no centralized authority acts as an agent for all communications; instead, each node is free to perform peer-to-peer functions known as transactions (Figure 1).

Blockchain is a decentralized architecture that features a distributed immutable ledger in which all transactions are recorded. More generally, blockchain is a secure and decentralized datastore of ordered records, including events, called blocks.[14] Each block consists of a group of transactions and a hash that binds it to the preceding block. These blocks are added to the blockchain through a majority node verification process known as a consensus protocol. The specific consensus protocol varies depending on the network. Once verified, the ledger is updated across all nodes in the network. The blockchain datastore is controlled by peers in the network and is independent of any third-party central management systems.

Although blockchain originated as the foundational technology that powers cryptocurrencies, such as Bitcoin and Ethereum,[14] it has since expanded to various other use cases, such as decentralized apps (DApps), blockchain voting, contract management, and identity management.[15]

PUBLIC AND PRIVATE BLOCKCHAINS

There are several distinctions between public and private blockchains, also known as permissioned and permissionless blockchain implementations. Public networks are accessible to every Internet user and do not discriminate based on credentials, location, or affiliation.[16] All participants are either pseudonymous or anonymous, and may add new blocks to the distributed ledger.[17] Any machine (with Internet access and the required

storage criteria) can become a node in the network, perform transactions, or view the public ledger. An example of a public blockchain is a cryptocurrency, such as Bitcoin and Ethereum. By contrast, private networks are centered around permissioned access of individual nodes. Users need credentials to connect to the network and these credentials are often provided for by a node already inside the network. Users are often labeled and identified and have restricted levels of access in the network based on its identification. There is a main identity provider that manages access control within the network, including control over users' ability to participate in the consensus protocol, query ledger data, perform certain transactions, and add new nodes. An example of a private blockchain is Hyperledger (https://www.hyperledger.org/).

RECENT MOVEMENTS IN PHARMACEUTICAL APPLICATIONS OF BLOCKCHAIN

There has been some discussion on the application of blockchain technology being in the pharmaceutical sector. According to the World Health Organization estimates, fake drug sales were worth as much as $75 billion in 2010, which makes the monitoring of drug transportation paths vital.[18] Given this situation, Lo and colleagues underscore the advantages of managing drug supply chains using a decentralized ledger technology.[18] They describe how blockchain implementations can provide visibility of vulnerabilities in the drug supply chain, where points of drug ownership transfer between pharmaceutical manufacturers, while other stakeholders have little visibility for tracking the authenticity of products. Engelhardt and colleagues[19] also suggested leveraging blockchain technologies to prevent prescription fraud by using it as a monitoring program to flag suspicious purchasing patterns and alert prescribers and pharmacists. Finally, Accenture recently released a white paper citing cold chain management as a target for blockchain implementations and how a decentralized ledger system could help with the complicated and expensive process of "temperature-controlled, refrigeration, production and distribution of products."[20] While the literature depicts opportunities for blockchain in the pharmaceutical sector, there are several deficiencies. First, there has been little focus on secure and trustworthy exchanges of personalized medication histories across healthcare institutions. Second, most of the work to date provided conceptual designs but did not provide the proof of concept.

CREATING A BUSINESS NETWORK VIA HYPERLEDGER FABRIC

Hyperledger Fabric is one of the Hyperledger projects founded by the Linux Foundation in 2015. It is an open-source blockchain framework tailored toward enterprise implementations. The Fabric development community currently has approximately 35 organizations and 200 developers.[21] A key advantage of Fabric is its modular architecture, which allows flexibility in a broad range of implementations including banking, finance, insurance, and healthcare. Its features provide support for pluggable consensus protocols, general-purpose programing languages for writing smart-contracts, and independence from native cryptocurrencies that require competitive mining. Fabric's smart contracts are implemented through chaincode, which is the business logic for transaction processes in the

network. Chaincode is highly programmable and can be structured for a variety of functions in the network.

Fabric uses the Practical Byzantine Fault-Tolerant consensus protocol,[22] which has several advantages over other protocols. First, nodes in a Practical Byzantine Fault-Tolerant system communicate with each other to agree on the state of the system at a specific time, such as verifying a new block. Second, it does not require a large amount of computational power to solve an intensive hashing algorithm, which is required in most public blockchain implementations and accomplished through proof of work. Proof of work has been widely used in cryptocurrencies (e.g., Bitcoin and Ethereum) to confirm transactions submitted to the network. In these cryptocurrency networks, machines participate in a process called cryptomining in order to generate the computational power needed for proof of work. By contrast, the Practical Byzantine Fault-Tolerant system consensus protocol does not rely on costly mining. Most notable for our implementation, Fabric is permissioned, meaning every user is vetted and therefore trusted in the network. In addition, permissioned chains use small consensus groups, resulting in a more efficient process of confirming the state of a new block.

Hyperledger Composer is an open development toolset for creating blockchain applications. The Composer supports the Fabric infrastructure and runtime and allows for quicker business network modeling, application implementation, and integration with existing systems.[23]

The Business Network Definition is exported as an archive (.bna file) when it is ready to be deployed. The definition of the network is made up of four main files: model, script, access control, and query (Figure 2).

The model file is responsible for outlining the structure of the network. It has three main components: assets, participants, and transactions. Assets are often the variables stored in the network. Participants are the nodes of the network and can interact with assets and other participants through transactions. Transactions are the functions of the network and are invoked to update the network (e.g., transferring an asset).

The *script file* defines the various transaction functions in the network. It is written in Javascript and handles the transaction logic, including which types of participants interact (different categories of participants have different levels of access in the network) and which types of assets are transferred.

The access control file delineates the specific scopes of access users have in the business network. This is where the role of the user (participant) is described, determining their role in creating, reading, updating, or deleting elements of the network.

The query file defines the structure and function of queries from this network. Queries can be defined to extrapolate transactions from the historian, which is a ledger of all past transactions in the network.

Once the network is defined, it can be exported as an archive, downloaded, and run on another machine. A network card is used to connect to the network. Network cards can take the form of a participant type or an admin (Figure 2). Participant cards generally have a more controlled scope of access in the network, while the admin can perform more high-clearance functions such as adding new participants or deleting participants. This card type defines the node that uses the card to connect to the network and, thus, outlines what kind of role the node plays.

BUILDING COMPONENTS OF THE BUSINESS NETWORK

Three main components of our Hyperledger Fabric network are shown in Figure 3. The network will be structured into participants, assets, and transactions. The network involves three parts: (1) prescribers who prescribe medications; (2) patients who receive the prescription; and (3) the details of the medication, such as the name, ingredients, and specific instructions for use. Because prescribers need to send the prescriptions to the network, prescribers will act as the nodes/participants in the network. Patients will not have permission to document prescriptions, but will have the right to provision access to their medication history to the prescriber/institutions of their choice. As such, patients and medication prescriptions will be assets and transactions in the network, respectively.

DMMS ARCHITECTURE

Figure 4 provides a high-level architectural depiction of DMMS. Each healthcare institutions has an administrator, a local network consisting of participants' accounts (prescribers), and asset accounts (patients). The global network is composed of all of the local networks, each of which is a part of the distributed ledger. A set of randomized nodes within each local network contains a copy of blockchain, which consists of all medication prescriptions ordered by participants within the global network. An healthcare institutions administrator (admin node) can create new participants and assets, which need to be validated by other institutional administrators. This ensures that the network cannot be tampered with even if an admin node is compromised. The newly created participants and assets will be updated across all nodes in the global network.

Each institution admin holds an administrative card to connect to the network. There may be multiple admin nodes in a single healthcare institution. Each prescriber will have a hospital computer associated with them, each of which will function as a participant node in the network. Machines will have a pre-installed client with a prescriber-type network card. Clients and network cards will be supplied by the institution admin. Prescribers will interact with the client interface, and the client will handle all the network connections and verification. The client holds a pair of keys to perform secure communications between prescribers and patients. Patients with an account issued by the admin will be provided a pair of private and public keys. The public key will be invoked to encrypt medication prescriptions, while the private key will be applied to decrypt the medication prescriptions they receive after querying the network's ledger.

CREATING TRANSACTIONS

In a medication prescription process, the patient will provide their public key to the prescriber to encrypt the prescription transaction. In a real-world implementation, patients will not need to memorize their public keys, but instead they use an online health portal to communicate their public key to the prescriber's machine or, alternatively, let the prescriber scan a Quick Response (QR) code (which will point to the public key). When a prescriber prescribes a medication, the prescriber client will assemble a transaction that consists of the prescriber ID, patient ID, details of medications (e.g., generic and brand names), their ingredients, instructions for how to use the medications (e.g. dosages and times per day), and the time the transaction was created. After the transaction is assembled, the client will use the patient's public key to encrypt the transaction and submit it to the ledger network. The network will package the transaction along with other new transactions to form a block and randomly select a set of nodes in the network to confirm the newly formed block. The workflow for submitting a medication prescription to the ledger network is depicted in Figure 5.

CONDUCTING QUERIES

In a query process, the prescriber will query all records under a patient using the patient ID. The records will include those submitted by the prescriber and all other healthcare providers who interacted with the patient. All the returned transactions will be decrypted with the patient's private key and the client will show the decrypted patient records.

The patient's private key should not be seen by or known to anyone else. To protect a patient's private key when transferred from one device to another, the following steps are taken. When a prescriber needs to query a patient's medication history, the prescriber sends an invitation to the patient through patient client. The patient must approve this invitation through their patient client (e.g., online health portal). The patient client generates a random salt value, combines it with their private key, and then encrypts the string with the prescriber's public key using an asymmetric encryption algorithm (e.g., Rivest, Shamir, and Adelman Encryption (RSA)). Next, the encrypted string is transferred to the prescriber client where it is decrypted with the prescriber's private key. The decrypted private key is then parsed from the string and used to decrypt the queried transactions. The process for a prescriber to query all medical prescriptions associated with a patient is depicted in Figure 6. An important distinction between the patient and prescriber clients constitutes the user interfaces. Patient clients will be built into their patient portals, while prescriber clients will be individual applications on their healthcare institution machines.

INTERPRETATIONS OF DMMS IN SECURITY, ACCESSIBILITY, AND PRIVACY

A decentralized ledger system has several advantages over a traditional third-party centralized system: security, accessibility, and privacy.

Security

In some breaches, intruders hold medical centers functionally hostage until a ransom is paid. These are known as ransomware attacks and are growing in prevalence.[24] Our decentralized network is resilient against ransomware and similar security breaches. This is because the decentralized network topology does not have a single point of failure or central repository for intruders to infiltrate. In the case where intruders infiltrate a single node in the network, they will be unable to read the ledger due to it being encrypted. Furthermore, the use of a private blockchain–hyperledger fabric adds an additional level of security because nodes must be approved from the institutional administrator, making it more difficult for invaders to create malicious nodes in a majority attack (e.g., where pool operators obtain control over the network once it injects over 50% of malicious nodes).[25] To learn health information, an attacker would need to bypass the initial institution firewall, infiltrate a majority of peer nodes, and decrypt industry standard encryption.

Accessibility

The DMMS should allow for easier access to medication records. Patients often have the burden of recalling their past medication history by memory or carry around physical copies of their medication records. Using the decentralized ledger system, prescribers can easily update medication histories through a simple client user interface. When patients visit different medical institutions, prescribers can query medication histories easily with the approval of the patient. The decentralized network eliminates the need to cooperate with a set of privatized central repositories.

Privacy

Barrows and colleagues explain that increasing reliability on centralized health data repositories leads to greater privacy risks.[26] Decentralized networks reduce the need for trust between the prescribers, patients, and the network.

INTEGRATION WITH EXISTING ELECTRONIC HEALTH RECORD SYSTEMS

There are several ways by which our system can be integrated into existing EHR infrastructure. For medication histories across healthcare institutions that use third-party EHR vendors (e.g., Epic or Cerner), Fast Health Interoperability Resource (FHIR) application programming interface can be used as bridges between the blockchain and EHR clients. Specifically, we recommend a data inquiry application program interface to pull health data from the patient's EHR and serve as initial entries for their medication histories. Future prescribed medications could then be pushed from our client to the EHR using the same FHIR application programming interface. A JavaScript Object Notation (JSON) format with *key*:*value* pairs could be used to define dynamic number of fields. Fields can include, but are not limited to, the product code, product code terminology (e.g., RxNorm), strength, dose form, quantity, quantity units, patient directions (sig), start and stop dates, number of refills, structured sig fields (e.g., dose, route, frequency, and pro re nata (PRN) indication), product status (e.g., active, on hold, completed, or canceled), and adherence.

On the prescriber's end, they only need to submit updates once because the client will handle the rest of the communications between the existing EHR and our DMMS network. This system would use standardized terminologies for coding drugs, including an identifier for which terminology was used. For example, care providers from some histories across healthcare institutions can use RxNorm ids and names, others may use Anatomical Therapeutic Chemical (ATC) classification system codes, while some others may use National Drug Code (NDC) codes. Regardless of which terminology is used, each transaction will contain original categories (RxNorm, ATC, or NDC).

PATIENT AND PRESCRIBER ACCEPTANCE

A potential barrier to this system is the requirement of patient health portals. Certain patient demographics (e.g., elderly or the mentally handicapped) may not have access to smartphones or may find it difficult to work with such systems. This may limit their ability to communicate with hospital clients for medication prescriptions. We believe that this problem can be addressed through in-hospital machines, where patients can log in to their account (possibly through the assistance of care providers) and manage their patient portals from there. Another solution could be for hospitals to include a QR code on the printed (or electronic) copy of the medication list at the end of an encounter for each patient. In doing so, a patient could browse and check his/her medication list. The QR code could store a patient's public key, which can be used by prescribers to access the medication list associated with the patient. If a patient has no Internet access at home or smartphone to manage security and privacy setting of their account, they can use hospital computers to manage them onsite. In addition, for patients who are unable to manage or use their health portals, current features in health portals such as allowing access to delegates or surrogates of patients address this issue.

One of the barriers to prescribers adopting our client is the potential increase in their workload. However, as alluded to earlier, the integration of FHIR application programming interface will alleviate this problem because it will allow for the simultaneous updating of the blockchain system and the EHR. Our prescriber client will be preinstalled in computers in each participating healthcare institutions, which will allow access to our client anywhere within an healthcare institutions. Still, it should be recognized that prescribers may need additional training when they first use our client. The training and learning process may add additional financial costs for healthcare institutions; however, there are many benefits to healthcare institutions for using our system. Beyond providing access to an accurate medication history, our system can also offer specific decision support to prescribers to avoid adverse drug reactions and replicated prescriptions. This could justify the time and cost spent on learning how to use and manage our client.

PROOF OF CONCEPT

As a proof of concept, we engineered a system to showcase the preliminary parameters involved in the prescriber client prescription process and a working decentralized network. The software is available as a GitHub project.[27]

As noted, Hyperledger Fabric serves as the network, while Hyperledger Composer handles simpler network modeling and integration with client applications. We used an Angular application hosted on a local machine to simulate the prescriber machine client and connected our client to the network through a RESTful application programming interface. The Hyperledger network was booted using command line. Figure 7 shows the prescriber client prescription and query process. The user interface is rudimentary and is only used to show the basic inputs needed by the prescribers for a prescription. The demo highlights the simplicity of this system—in just two steps, a prescriber can prescribe medication and then query the record regardless of institution affiliation.

IMPLICATIONS OF DMMS IN E-PRESCRIBING

The rate of e-prescribing increased drastically when the Medicare Improvements for Patients and Providers Act began offering financial incentives for institutions to use e-prescribing in 2008. By 2014, 70% of prescribers were e-prescribing on the Surescripts network,[28] and now e-prescribing is almost ubiquitous. The current e-prescription process relies on centralized third-party systems to connect pharmaceutical companies with healthcare institutions. Figure 8 shows the workflow of a typical e-prescription process.

To begin, prescribers write prescriptions in their institution's EHR system. The prescription is then e-prescribed to a pharmacy via an e-prescribing central network such as the Surescripts network, and the patient picks up their medication at the pharmacy. The pharmacy dispensing and pharmacy benefit manager (PBM) claims data are then sent back to the e-prescribing central entity (e.g., Surescripts) by participating pharmacies, payers, and PBMs; however, not all pharmacies, payers, or PBMs participate in dispense data sharing.[29]

Reliance on centralized networks allows for a single point of failure in the e-prescription process, imbues high costs on histories across healthcare institutions, and generally complicates the e-prescription process. For instance, Surescripts needs to coordinate between histories across healthcare institutions and pharmacies to ensure that their information can be exchanged with each other. When the number of involved institutions increases, the complexity to deal with such coordination will exponentially increase, and subsequently the costs will rise. Another limitation is that healthcare institutions and pharmacies must place trust in Surescripts that the e-prescriptions are accurate; however, errors such as the misidentification of patients are not uncommon when using such services.[30] In addition, pharmacy claims data (and commonly pharmacy dispense data by Surescripts) do not include dose, route, frequency, or additional patient instructions.[31]

As shown in Figure 9, a decentralized solution can greatly simplify the e-prescription process by eliminating the middleman and allowing safe communications directly between histories across healthcare institutions and pharmacies. Our ledger solution can be expanded to include e-prescriptions by adding an e-prescription transaction function and installing a client in all participating pharmacies. Our solution ensures that e-prescriptions can be accessed and exchanged among participants (e.g., prescribers and pharmacists) without relying on any central servers. At the same time, participants do not need to rely on a central system to build trust between each other. Each e-prescription managed in our blockchain is

inherently trustworthy. Finally, patients can control which participants have accesses to their e-prescriptions because each e-prescription transaction would be encrypted using a patient's public key such that only the patient's private key could be used to decrypt the transaction.

It is notable that each transaction submitted to the network and confirmed by peers cannot be altered by anyone else, which would likely reduce e-prescription errors (e.g., misidentification and content alterations) during the transactions. Additionally, this would greatly facilitate prescription transfers between pharmacies and reporting to controlled substance prescription drug monitoring programs (PDMPs). Our solution can also overcome problems of trustworthiness and security raised by electronic prescriptions for controlled substances (EPCS), which was legalized by the US Drug Enforcement Administration (DEA) and aims to address the problem of prescription drug abuse in the United States.[32] It is not uncommon for prescriptions to be forged or stolen under the current EPCS technology, which heavily relies on a centralized network to require authentication of prescribers, and audit EPCS.[33] As mentioned earlier, e-prescription errors such as misidentification of patients and prescribers are hard to prevent in centralized systems; thus, our decentralized ledger solution provides a great opportunity to satisfy EPCS's requirements of trustworthiness and security.

CONCLUSIONS

In this article, we introduced a framework for a decentralized ledger system to medication history management to be more robust, secure, and convenient. We further detailed the architecture of our framework, showcased a demonstration network as a proof of concept, and analyzed ways for its implementation in the e-prescription industry. We highlighted the current difficulties in transferring medication data and the unsecure nature of centralized networks and explained how our solution can address these issues.

This framework is notable but has room for expansion in several ways. First, our system can be integrated with existing ADE research to provide decision support for prescribers based on the history of a patient's medications. Second, in addition to tracking prescriptions, our network can also be used as a standardized system for patient reported results. This can be achieved by increasing the functions of a patient's client to allow them to submit transactions (e.g., ADEs or medication consumption confirmations).

Funding Statement

This research was funded by the Vanderbilt Academic Support Program.

REFERENCES

1. Fung KW, Kayaalp M, Callaghan F, McDonald CJ. Comparison of electronic pharmacy prescription records with manually collected medication histories in an emergency department. Ann Emerg Med. 2013;62(3):205–11. [PubMed: 23688770]
2. Glintborg B, Andersen SK, Poulsen HE. Prescription data improve the medication history in primary care. Qual Saf Health Care. 2010 6;19(3):164–8. 10.1136/qshc.2008.029488 [PubMed: 20194218]

3. Tam VC, Knowles SR, Cornish PL, et al. Frequency, type and clinical importance of medication history errors at admission to hospital: A systematic review. CMAJ. 2005 8 30;173(5):510–15. [PubMed: 16129874]
4. Bates DW, Boyle DL, Vander Vliet MB, Schneider J, Leape L. Relationship between medication errors and adverse drug events. J Gen Intern Med. 1995 4;10(4):199–205. [PubMed: 7790981]
5. Agency for Healthcare Research and Quality. Reducing and preventing adverse drug events to decrease hospital costs. Research in Action. 2001 Available from: http://archive.ahrq.gov/research/findings/factsheets/errors-safety/aderia/ade.html (accessed July 23, 2018)
6. Forster AJ, Murff HJ, Peterson JF, Gandhi TK, Bates DW. Adverse drug events occurring following hospital discharge. J Gen Intern Med. 2005 4;20(4):317–23. [PubMed: 15857487]
7. Joint Commission on Accreditation of Healthcare Organizations. Using medication reconciliation to prevent errors. Sentinel Event Alert. 2006;35:1.
8. Seymour RM, Routledge PA. Important drug-drug interactions in the elderly. Drugs & Aging. 1998;12:485 10.2165/00002512-199812060-00006 [PubMed: 9638396]
9. Norén GN, Sundberg R, Bate A, Edwards IR. A statistical methodology for drug-drug interaction surveillance. Stat Med. 2008 7 20;27(16):3057–70. 10.1002/sim.3247 [PubMed: 18344185]
10. Schmiedl S, Rottenkolber M, Hasford J, et al. Self-medication with over-the-counter and prescribed drugs causing adverse-drug-reaction-related hospital admissions: Results of a prospective, long-term multi-centre study. Drug Saf. 2014 4;37(4):225–35. 10.1007/s40264-014-0141-3 [PubMed: 24550104]
11. Bitglass. (n.d.). Number of healthcare data breaches in the U.S. from 2014 to Q1 2017, by breach type. In Statista—The Statistics Portal. Available from: https://www.statista.com/statistics/798588/number-of-us-healthcare-data-breaches-by-type/ (accessed August 10, 2018)
12. 5 Epic contracts—and their costs-so far in 2016. (n.d.). Available from: https://www.beckershospitalreview.com/healthcare-information-technology/5-epic-contracts-and-their-costs-so-far-in-2016.html (accessed June 24, 2018)
13. Hatch J, Becker T, Fish JT. Difference between pharmacist-obtained and physician-obtained medication histories in the intensive care unit. Hosp Pharm. 2011;46(4):262–268. 10.1310/hpj4604-262
14. Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. Trials. 2017 7 19;18(1):335 10.1186/s13063-017-2035-z [PubMed: 28724395]
15. Salviotti G, De Rossi LM, Abbatemarco N. A structured framework to assess the business application landscape of blockchain technologies Proceedings of the 51st Hawaii International Conference on System Sciences. 2018. 1 3–6, 2018; University of Hawai'i at Manoa; Hilton Waikoloa Village, Hawaii.
16. Olleros FX, Zhegu M Research handbook on digital transformations. Cheltenham, UK: Edward Elgar Publishing; 2016 ISBN-13: 978–1784717759. ISBN-10: 17847177544
17. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain In AMIA Annual Symposium Proceedings. American Medical Informatics Association 2017; 650 Washington D.C.
18. Lo C Blockchain in pharma: Opportunities in the supply chain. Available from : https://www.pharmaceutical-technology.com/digital-disruption/blockchain/blockchain-pharma-opportunities-supply-chain/ (Accessed August 06, 2018)
19. Engelhardt MA. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technol Innovation Manag Rev. 2017;7(10):22–34. 10.22215/timreview/1111
20. Carly G, Matthew P, Nishant M. In blockchain we trust: Transforming the life sciences supply chain [White Paper]. 2018 [cited 2018 Aug 15]. Accenture Life Sciences. Available from: https://www.accenture.com/t20180409T144103Z__w__/cz-en/_acnmedia/PDF-71/Accenture_Blockchain_Innovations_Life_Sciences.pdf
21. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, 2018 4 23–26;30:1–30:15 10.1145/3190508.3190538
22. Castro M, Liskov B. Practical Byzantine fault tolerance. OSDI. 1999;99:173–86.

23. Welcome to Hyperledger Composer. (n.d.). Available from: https://hyperledger.github.io/composer/latest/introduction/introduction.html (Accessed July 06, 2018)
24. Tuttle H Ransomware attacks pose growing threat. Risk Manag. 2016;63(4);4–7. Available from: http://login.proxy.library.vanderbilt.edu/login?url=https://search.proquest.com/docview/1792354247?accountid=14816 (Accessed June 16, 2018)
25. Bastiaan Martijn (2015): Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin. Available from: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf (Accessed June 10, 2018)
26. Barrows C, Clayton PD. Privacy, confidentiality, and electronic medical records. JAMIA. 1996;3(2):139–48. 10.1136/jamia.1996.96236282 [PubMed: 8653450]
27. Patrick L (n.d.). LiPatrick/decentralized-med-network. 2018 Available from: https://github.com/liPatrick/decentralized-med-network
28. Gabriel MH, Swain M. E-Prescribing trends in the United States ONC Data Brief 2014 no.18. Washington, DC: Office of the National Coordinator for Health Information Technology.
29. Frisse ME, Tang L, Belsito A, et al. Development and use of a medication history service associated with a health information exchange: Architecture and preliminary findings. AMIA Annual Symposium Proceedings. American Medical Informatics Association. 2010;2010:242–5.
30. Odukoya OK, Stone JA, Chui MA. Barriers and facilitators to recovering from e-prescribing errors in community pharmacies. J Am Pharm Assoc. 2015;55(1):52–8.
31. Phansalkar S, Her QL, Tucker AD, et al. Impact of incorporating pharmacy claims data into electronic medication reconciliation. Am J Health Syst Pharm. 2015 2 1;72(3):212–17. 10.2146/ajhp140082 [PubMed: 25596605]
32. Drug Enforcement Administration. Electronic prescriptions for controlled substances. Federal Register 2010 Available from: http://www.federalregister.gov/articles/2010/03/31/2010-6687/electronicprescriptions-for-controlled-substances Accessed August 10, 2018
33. Hufstader GM, Yang Y, Vaidya V, Wilkins TL. Adoption of electronic prescribing for controlled substances among providers and pharmacies. Am J Manag Care. 2014 11;20(11 Spec No. 17):SP541–6. [PubMed: 25811828]

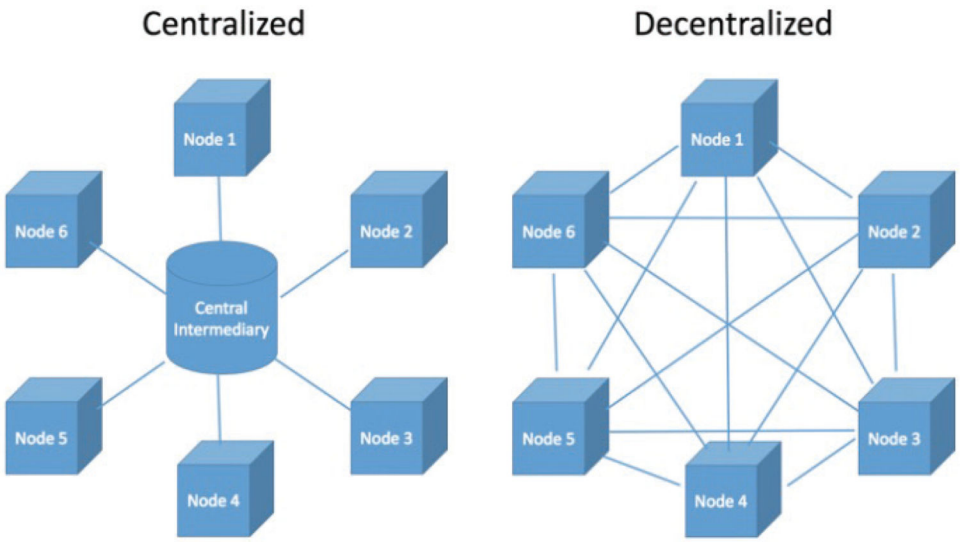

Figure 1—.
Network structures of centralized system (left) and decentralized system (right).

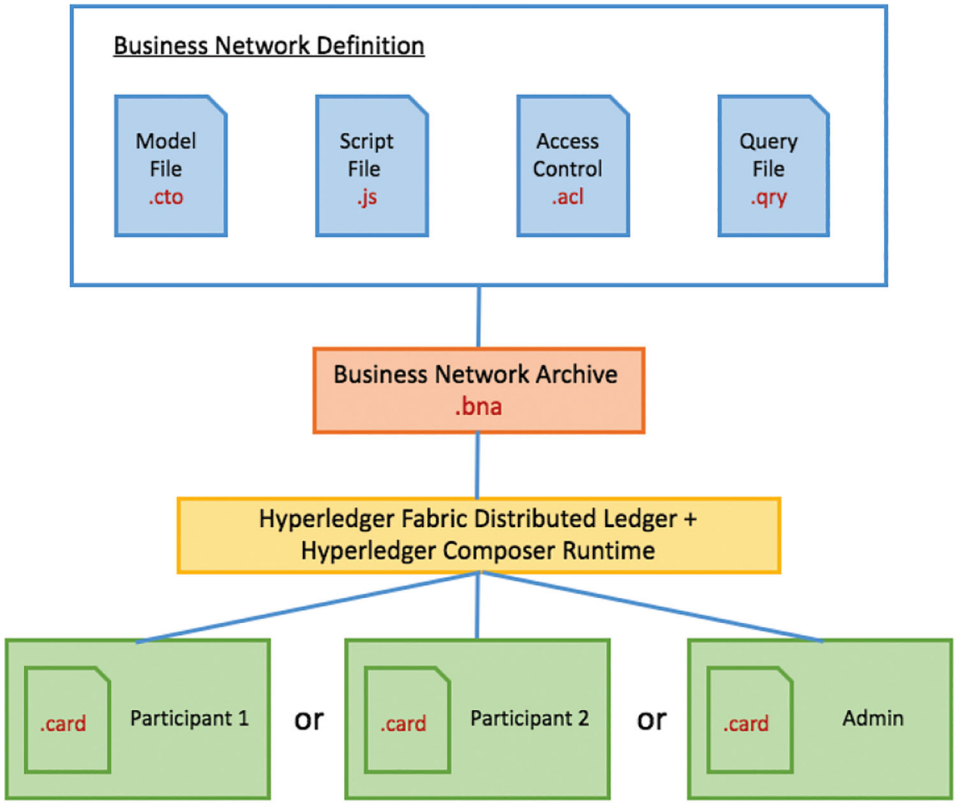

Figure 2—.
A framework to create a network via Hyperledger Composer.

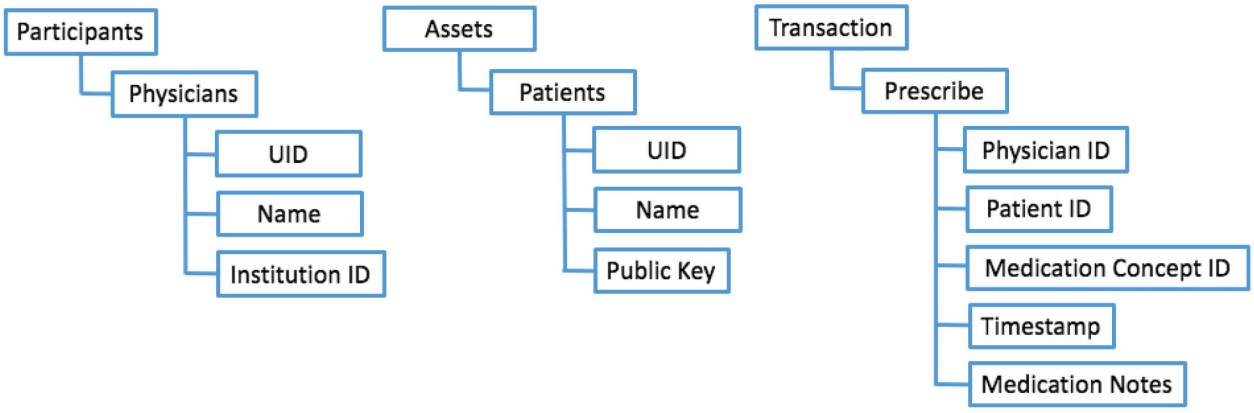

Figure 3—.
Three components of the Hyperledger Fabric-based business network.

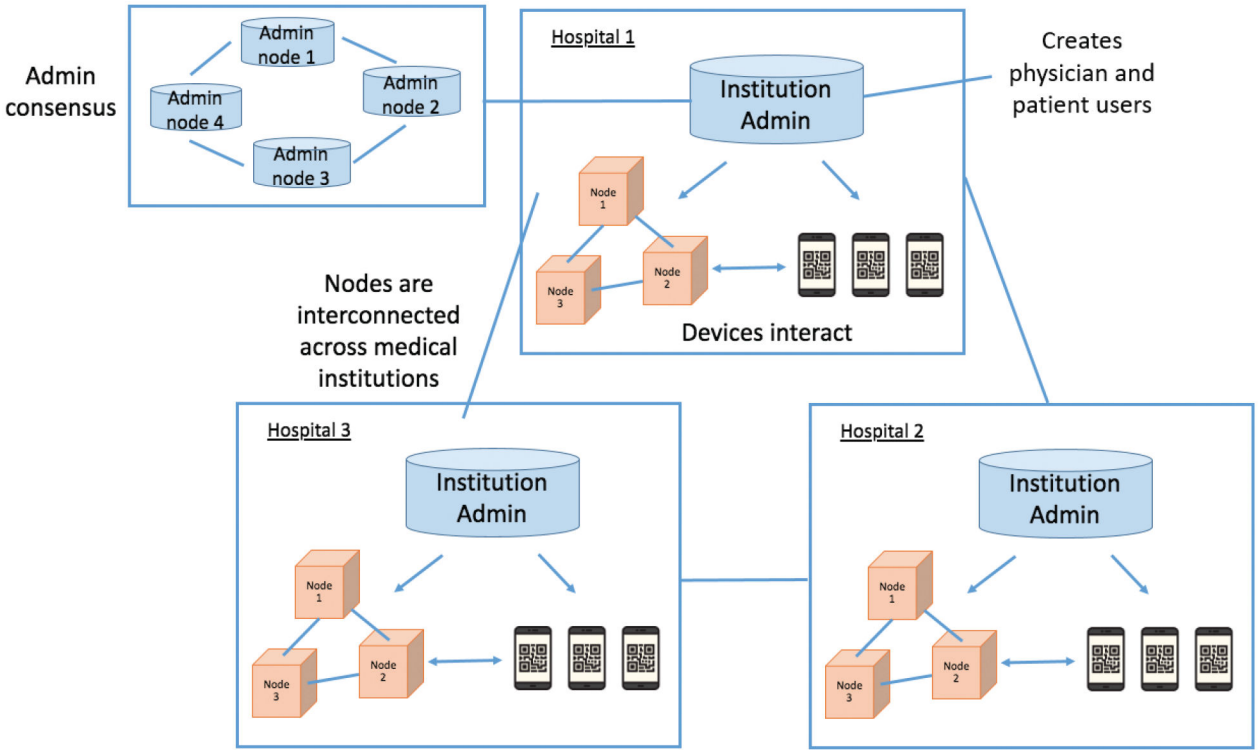

Figure 4—.
Architecture of decentralized ledger system applied across several healthcare institutions.

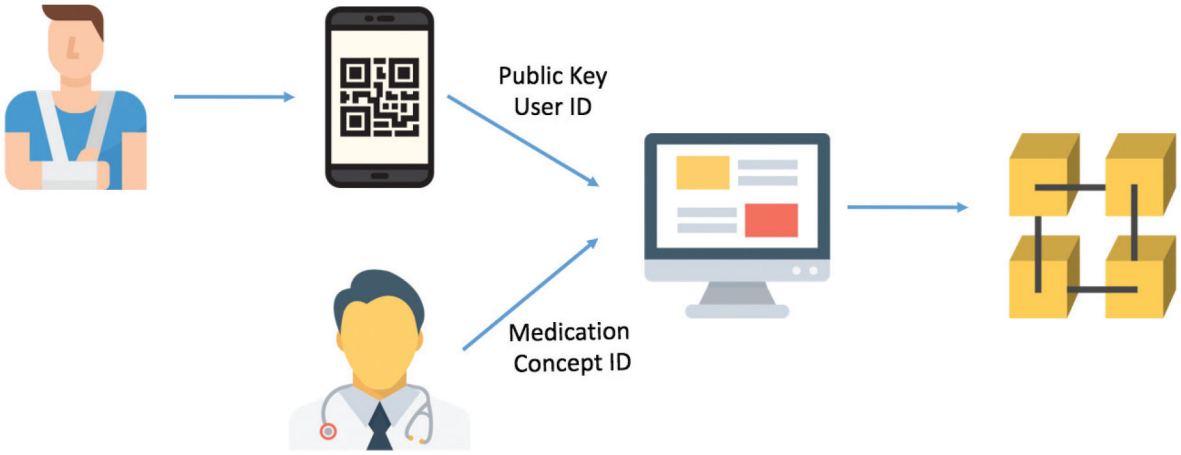

Figure 5—.
Workflow for the submission of a medication prescription to the ledger network.

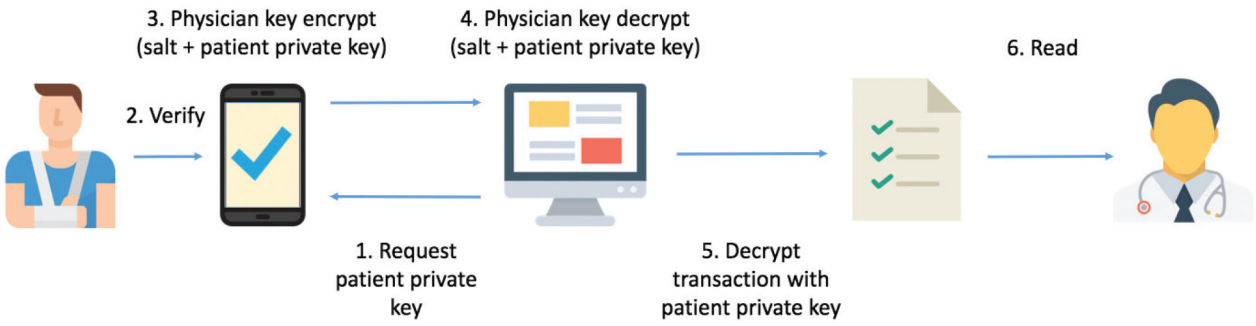

Figure 6—.
A workflow for a prescriber to read all medical prescriptions associated with a patient.

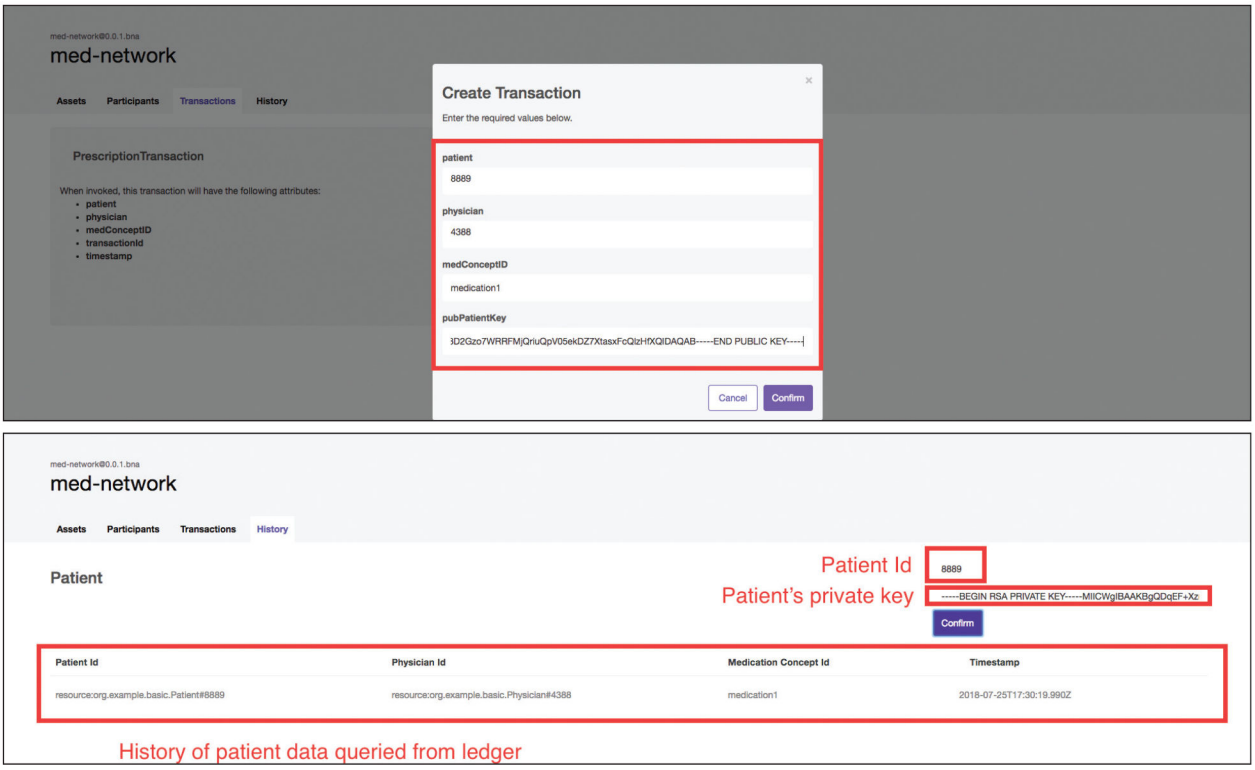

Figure 7—.
Screenshots from the prescriber client view in our demo system.

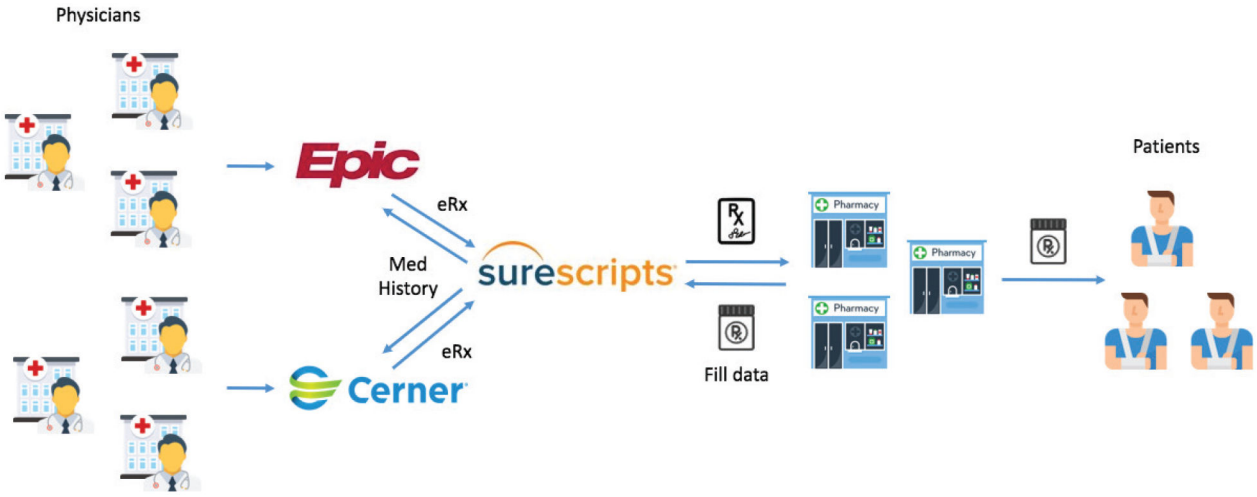

Figure 8—.
E-Prescription process with centralized system.

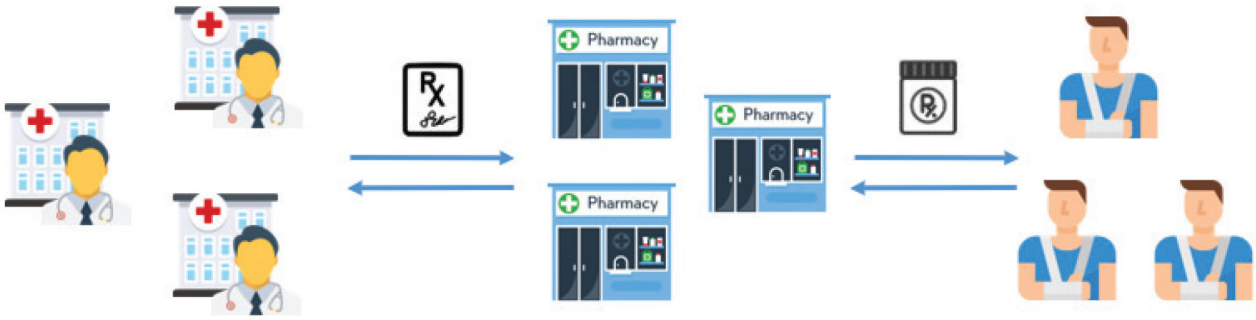

Figure 9—.
E-Prescription process with decentralized system.