*JAMIA Open*, 00(0), 2021, 1–8
doi: 10.1093/jamiaopen/ooaa073
Research and Applications

Research and Applications

# Designing and testing a blockchain application for patient identity management in healthcare

**Anjum Khurshid[1], Cole Holan[1], Cody Cowley[1], Jeremiah Alexander[1], Daniel Toshio Harrell[1], Muhammad Usman[2], Ishav Desai[1], John Robert Bautista[3], and Eric Meyer[3]**

[1]Department of Population Health, Dell Medical School, The University of Texas at Austin, Austin, Texas, USA, [2]Cockrell School of Engineering, The University of Texas at Austin, Austin, Texas, USA and [3]School of Information, The University of Texas at Austin, Austin, Texas, USA

Corresponding Author: Anjum Khurshid, MD, PhD, Department of Population Health, Dell Medical School, The University of Texas at Austin, 1701 Trinity Street, Austin, TX 78712, USA; anjum.khurshid@austin.utexas.edu

Received 3 August 2020; Revised 25 November 2020; Editorial Decision 20 December 2020; Accepted 23 December 2020

**ABSTRACT**

**Objective**: Healthcare systems suffer from a lack of interoperability that creates "data silos," causing patient linkage and data sharing problems. Blockchain technology's unique architecture provides individuals greater control over their information and may help address some of the problems related to health data. A multidisciplinary team designed and tested a blockchain application, MediLinker, as a patient-centric identity management system.

**Methods**: The study used simulated data of "avatars" representing different types of patients. Thirty study participants were enrolled to visit simulated clinics, and perform various activities using MediLinker. Evaluation was based on Bouras' criteria for patient-centric identity management and on the number of errors in entry and sharing of data by participants.

**Results**: Twenty-nine of the 30 participants completed all study activities. MediLinker fulfilled all of Bouras' criteria except for one which was not testable. A majority of data errors were due to user error, such as wrong formatting and misspellings. Generally, the number of errors decreased with time. Due to COVID-19, sprint 2 was completed using "virtual" clinic visits. The number of user errors were less in virtual visits than in personal visits.

**Discussion**: The evaluation of MediLinker provides some evidence of the potential of a patient-centric identity management system using blockchain technology. The results showed a working system where patients have greater control over their information and can also easily provide consent for use of their data.

**Conclusion**: Blockchain applications for identity management hold great promise for use in healthcare but further research is needed before real-world adoption.

**Key words:** blockchain, identity, mobile application, health information, patient consent

## INTRODUCTION

Electronic medical records (EMRs) contain an individual patient's highly sensitive private information including identifying information and personal medical records. However, these EMRs are created, maintained, and stored across multiple isolated hospitals and healthcare providers creating "data silos" that cause major patient linkage and data sharing problems in healthcare (1). The 21st Century Cures Act, 2016 has mandated the federal government to

**LAY SUMMARY**

A multidisciplinary team designed and tested a blockchain application, MediLinker, as a patient-centric identity management system. MediLinker uses blockchain technology's unique decentralized identity architecture to provide individuals greater control over their information. We used simulated data of "avatars" representing different types of patients to test the functionality of MediLinker in a patient's journey through a health system. Thirty study participants were enrolled to visit simulated clinics and perform various activities typical to a patient's interactions in clinical settings. Evaluation was based on Bouras' criteria for patient-centric identity management and on the number of errors in entry and sharing of data by participants. The study demonstrated that MediLinker gave patients the ability to use validated identity to check-in at clinics, to share their personal information, to withdraw permission, and to make changes to their personal data. This evaluation provides evidence of the potential use of a blockchain-based, patient-centric identity management system in healthcare settings, where patients have greater control over their information and can easily share their data for clinical and research purposes.

find ways to make access to patient data "easy." The distributed nature of blockchain technology can bridge the existing "data silos" across health systems and bring the patient to the center of healthcare identity and information management (2, 3).

There has been growing support for demands to put individuals in control of their personal information and to build a system that is based on the individual's control and consent (4). Patient engagement has been promoted through patient portals and view, download, and transfer (VDT) requirements in meaningful use, yet most patients do not have easy access to their medical records (5). Establishing a system that gives patients control of their own data is not only going to be extremely expensive with existing health information infrastructure but also will likely require a long time.

Blockchain technology is based on the principle of providing an individual control over their data and information, and hence potentially appropriate as part of a solution to patient ownership of their health data. There are 3 key benefits to blockchain technology's use in healthcare that relate to the patient. First, blockchain is able to create a decentralized identification (DID) that allows health care providers and patients to interact with one another directly without the need for an intermediary (2, 6, 7). The second key benefit is the immutable audit trail which allows all changes of personal information to be tracked and traced (2). The third benefit is the increased security of patients' medical information. Not only is the data stored in multiple nodes across the distributed ledger; but it also is encrypted with the only key being in the hands of the patient (2, 8). Blockchain applications may, therefore, provide solutions to the current problems of interoperability of medical records, incomplete patient data at the point of service, and lack of access to personal records while ensuring security (9, 10).

Currently, practical aspects of blockchain applications in healthcare are poorly understood. There has been limited evaluation of how blockchain systems will work in a real-world healthcare environment. One real-world situation where prior work has shown the potential of this technology is for addressing the lack of transaction identity in homeless populations (11). However, this study showed that privacy, data security, usability, and adoption by providers and consumers is still hard to test using real patient data in order to follow the "do no harm first" principle (12). Due to rapid evolution of blockchain applications and faster rate of adoption in other industries, it is possible that blockchain applications may be pushed into healthcare practice without adequate research and evaluation. A search of MEDLINE shows that the number of papers on blockchain applications in healthcare are limited and in fact were almost nonexistent before 2018 (13).

We describe the design, development, and testing of a patient-centric blockchain identity and consent management system for patients, called *MediLinker*, in a simulated environment on a large residential urban university campus. The simulated environment allowed us to test a variety of healthcare scenarios and focus on the system's performance for identity and consent management while minimizing the risk to human subjects. The purpose of the study is to test the functionality of the blockchain-based identity and consent management application, and not the attitude and behavior of individuals whose personas are used for testing the various features of the application. This article describes the process we adopted, implementation of MediLinker, and results of its evaluation.

## METHODS

Below we describe in more detail the MediLinker system, our study design, recruitment of participants, implementation, and evaluation methodology.

### MediLinker system

The MediLinker system was designed with certain features in mind:

- to allow patients to be able to prove their identity and receive healthcare services without having to carry identification to each visit and service location;
- to allow patients' detailed control over what information they would like to share with different providers;
- to develop a system where every use of the patient information requires their consent, provided electronically;
- to share medical records, insurance details, identity details, and credit card information through the system;
- to ensure patient's information is secure, confidential, and auditable.

The MediLinker platform was built using Hyperledger Indy, which is a blockchain platform specifically developed to facilitate distributed transaction identity management. Hyperledger Aries was used as an API (application programming interface) to connect HyperLedger Indy's identity management features and personalized encrypted digital wallets, stored on an individual's mobile device. A crypto wallet, only accessible to the patient through a private key, holds patient-level personal information and not stored per se on the blockchain network. Only when the patient provides consent through use of their private key, any data from the wallet is shared on the secure blockchain network with another node. While some other blockchain platforms (like Ethereum, uPort) could have been

used for developing such an identity management solution, we selected Hyperledger Indy as our development platform because it is based on W3C (World Wide Web Consortium) standards, supports DIDs in a way that provides full autonomy to users over their data, and has an active and supportive user community.

## Study location

The study was designed to use simulated data and create 'avatars' representing different types of patients. Study location was the University of Texas at Austin campus, which facilitated recruitment of students and avoided logistical challenges. To comply with HIPAA (Health Insurance Portability and Accountability Act) and FERPA (Family Educational Rights and Privacy Act) requirements related to both personal and educational data, no personally identifiable information from the participants was used. The study also required establishment of simulated clinic sites to test registration, consent, and data sharing. Study sites were modified, as described later, due to external circumstances which prevented in-person interactions on campus. The second part of the study was, therefore, conducted online.

## Participant recruitment

Four academic units on campus were identified for recruitment purposes based on convenience and representation on the project team. We used posters, email listservs, and personal contacts to recruit students in each unit. The recruitment advertisements were sent on January 6, 2020 and closed on February 7, 2020. Participants were assigned at random to the 2 waves or sprints of the study before February 20, 2020.

A total of 30 students were recruited. Each participant was paid $170, in 3 installments, for completion of the study. The study participants eligibility criteria were:

- 18–35 years old
- Any gender
- University of Texas at Austin registered student
- Willing to follow the study protocols
- Able to visit identified locations twice a week
- Participate in evaluation activities

The study was deemed by the Institutional Review Board as non-human subjects research.

## Study design (sprint 1 and 2)

A study design was developed by an interdisciplinary team that included researchers from the Medical School, School of Engineering, IT Services, and the School of Information. To simulate real-world scenarios, we identified convenient locations on campus as "clinics" for patient visits. We also included a special case of a research center that used patient data for clinical research.

The simulated clinics were as follows:

1. Community Clinic
2. Acute Care Clinic
3. Psychology Clinic
4. Rehabilitation Clinic
5. Austin Community Health Research Center

The study included patients initially enrolling in one clinic and later visiting another clinic at another location on campus. These clinics were conveniently located on campus but had totally separate information systems that did not connect to each other thus simulating a patients' journey through different health systems. These clinics could have been physically located anywhere in the city, state, or the country for testing the application. Using the MediLinker application the patient could share their personal information in a secure and verified manner without having to show their identity at any time after the first verification. The patient would also be able to choose granular data to be shared upon request and also allow, for instance, a research center to get consent for using the patient's medical data for research. The study design demonstrated how a blockchain-based system could allow the patient to share granular data with other clinics or a research center in a live mode.

**Table 1.** Avatar profiles created

| Use case | Key Bouras' criteria tested in the use case |
|---|---|
| Male adult patient | Autonomy, Approval, Authority |
| Female adult patient | Autonomy, Approval, Authority |
| Patient <21 year old | Interoperability |
| Patient with sensitive health information | Confidentiality |
| Patient missing medical history and credit card | Availability, Approval |
| Patient without insurance | Availability |
| Patient experiencing homeless | Availability |
| Undocumented immigrant | Availability |
| Bad Actor (trying to steal other's medical information) | Confidentiality |
| Bad Actor (using other's medical information as benevolent actor) | Confidentiality |

The 30 participants recruited for the study were split into 2 groups of 15 with each being assigned a particular avatar (Table 1). See Figure 1 for an example of the scripts developed to describe avatars. This script was provided to a participating student who acted as one of the fake patients during the testing of MediLinker and followed step-by-step instructions.

At the start of the study, each participant was given a folder with details of their avatar and a new email account was created for it. The information provided to each avatar consisted of:

- Fake driver's license with name, address, date of birth, etc.
- Fake credit card information with card number, expiration date, security code, and home address
- Fake health insurance card information, using standard health insurance format
- Fake medical record information including drugs currently prescribed

Study participants were asked to use this information during scheduled visits to various clinics and enter this information into MediLinker as described in the instructions for their avatar.

## Study use cases

We used the theoretical framework developed by Bouras to test how MediLinker can fulfill the criteria of identity management as described in the framework (14). Fifteen use-case avatars or artificial patient profiles were used to test MediLinker's ability to handle 6 of the 7 criteria of identity management identified by Bouras: Autonomy, Authority, Availability, Approval, Confidentiality, and Interoperability (Table 1). Tenacity, the seventh criteria, was not tested in this study as it requires longitudinal data over the lifespan of a patient. These avatars were designed to capture different types of

Sample Avatar-1: 44 year old male undocumented immigrant

Backgrouond: Jose immigrated to the United States in May of 2009. He has been working for some time as freelance help and recently got a job as a chef at a burger shop in Louisiana. He recently moved and is now working in Austin at a Burger Joint on South Lamar. He has four kids and works hard to supply their basic needs – some of Jose's favorite things include watching Soccer and playing with his kids. While living in the US Jose has made good friends and is well connected within his community – whenever he has financial or social problems, he relies heavily on his neighbors and friends for support and guidance. Rarely, if ever, does Jose use the healthcare services as he is scared of being deported – he has found some help at a community clinic that does not check documentation. Recently, Jose was diagnosed with Guillain-Barre Syndrome as a consequence of *Campylobacter jejuni* infection. Jose is worried as his symptoms are getting worse (ascending paralysis starting in the feet) and he needs to continue to work to support his family. Jose does not have an official US ID of any sort. All he has is a photo ID from his gym membership.

Week 1: Visit Acute Care Clinic for initial verification and simple-check in
Week 2: Visit Psych Clinic and share all of your profile information except 'medical history'
Week 3: Visit Community Clinic refuse sharing of any information, but still check-in
Week 4: Accept the offer to be part of a research trial

Sample Avatar2: 21 year old female adult

Background: Amy attends the University of Texas where she studies communication. She exercises at least three times per week. In addition, she goes jogging around Lady Bird Lake fairly frequently as well. She tries to eat mainly healthy food - whether that's salads or low fat foods. She has diabetes type 2 and regularly gets medication at a clinic in North Austin because that's where her family lives. However, she has begun to look for a new clinic to travel to because getting to North Austin is difficult due to her heavy involvement in organizations around campus. She asks Mary Gown to pick up her insulin for the week when she was too busy with classes to make it to the clinic to pick them up.

Week 1: Visit Community Clinic for initial verification and simple check-in
Week 2: Visit Acute Care Clinic, because Community Clinic is too far, and share all your profile information
Week 3: Amy cannot go to pick refill, so Mary Gown picks up Amy's Meds at the clinic
Week 4 Research – you receive invite from Austin Community Health Research Center to participate in a study about effects of blood type and hemoglobin A1c levels. You add the Center to MediLinker with permission to share your data for research.

**Figure 1.** Example of some avatars used in the MediLinker study.

patients frequently seen in the community with particular focus on certain vulnerable populations like the homeless or undocumented immigrant. Each avatar had some overlapping and other unique tasks to perform. While all of them tested the basic identity verification tasks, different avatars also covered unique aspects of the Bouras' criteria in our observations, as shown in Table 1. We also added 2 profiles or avatars of "bad actors" who might want to use the system unlawfully or without permission.

Bouras' framework was applied to the use cases as follows:

- Autonomy was tested by enabling patient identity to be independent of the identity provider or central governor.
- Authority was tested by evaluating if participants were able to control their data and EHR accounts without compromise throughout the study.
- Availability was tested by whether the information was accessible throughout the study's duration to the participants.
- Approval was determined by whether patients could approve or deny changes to their account information.
- Confidentiality was provided by allowing patients to revoke or redact information at any moment throughout the study.
- Interoperability was tested by allowing patients to share information from one healthcare clinic to another.

We also tested various clinical scenarios using the MediLinker system. These scenarios included simple enrollment at a clinic as well as consent for sharing information with another clinic. In total 6 scenarios were tested by different avatars during the implementation of MediLinker in the 4 clinic locations:

1. Initial enrollment at first clinic using a validated health identity (such as a driver's license)
2. Enrollment at a second clinic with only MediLinker to show valid health identity
3. Consenting and sharing personal/medical data between clinics
4. Withdrawing full/partial consent for sharing data between clinics
5. Changing personal information on blockchain wallet and validating the modification
6. Consent to participate in research projects

### Study implementation

The study was implemented in 2 separate "sprints" of 4 weeks with 6 in-person visits by each participant. Each week, the participants received detailed guidelines for their patient character or "avatar" via email. Instructions included clinical updates for the avatar, information sharing within and between the simulated clinics and changes to personal data. Instructions asked participants to visit a specific clinic to update their patient information in accordance with the guidance found within the emails. Each avatar had a unique role that tested a specific aspect of MediLinker, testing functionality, and usability.

During the first 3 weeks of each sprint, avatars were required to visit a clinic an average of 2 times per week. These visits typically consisted of checking-in to a clinic, entering new information into one's profile, removing information from one's profile, editing current information within one's profile, and checking-out of the same clinic.

*Sprint 1: In-person at physical clinics on UT Campus (February 24, 2020 to March 27, 2020)*. The first sprint was carried out entirely in-person with the various clinics arranged on UT Austin's campus. The participants were unaware of MediLinker's use of blockchain to establish a baseline of participants' attitude toward blockchain in healthcare.

*Sprint 2: "Virtual" clinics over Zoom (April 6, 2020 to May 5, 2020)*. In contrast, the 15 participants in sprint 2 were informed that the underlying platform uses blockchain technology. This approach evaluated whether the knowledge of a blockchain framework affects participant's usage of the system or concerns. Due to the COVID-19 pandemic we had to adjust our implementation to avoid face-to-face interactions. We changed the implementation plan, with approval of the IRB, to test the avatar use cases in "virtual" clinics over Zoom, allowing for a test of blockchain in a telemedicine context.

### Assessing feasibility: sprint 1 versus sprint 2

We assessed MediLinker's feasibility as an electronic verifiable healthcare identification management system using the following:

1. Participants' ability to create a validated profile
2. Accuracy of participants' data entries
3. Participants' ability to share their profile with multiple healthcare entities.

We identified different user errors and measured how many participants made which error. The user errors were classified into the following categories:

- formatting: participants did not format the dates or addresses according to what was provided to them
- misspelling: participants misspelled any item while entering profile data
- incorrect data entry: participants entered incorrect data, for example, credit card number, dates, etc.
- shared data with wrong clinic: participants made mistakes in using drop down menus to share data with another clinic
- data not shared: participants failed to share data

Errors were detected by recording each avatar's responses and comparing the expected results to the observed results. A chi-squared test was used to determine the significance between sprint 1 (in person, $n = 88$) and sprint 2 (virtual clinics, $n = 95$). Interoperability was evaluated using a multitude of factors: calculating the number of successfully shared data encounters, successful use of verified account information to visit a new clinic without needing to reverify, and number of research recruitment invites successfully received by participants.

### Ethical considerations

We created simulated patient identities to avoid any risk for actual data of a patient being used for this research. We also included use cases of vulnerable and underserved populations to allow for diversity of use cases. Participants' private information was not used, hence the study was considered nonhuman subjects by the Institutional Review Board.

## RESULTS

Twenty-nine out of 30 enrolled participants completed the study. The one drop out was for nonresponse. There was a gap of 2 weeks between recruitment and implementation that may explain the single drop out. All other participants were responsive to weekly surveys, appeared at clinic locations as directed, and completed all steps identified in the study protocol. Clinic visits and sprints were organized on a calendar to manage the study participants and match them with the use cases and clinics according to the study design. All interactions of the avatars with MediLinker were captured electronically and analyzed against the criteria developed by Bouras to measure user-centric identity management. The results of the testing are shown in Table 2.

Data regarding error rates by participants in completing various tasks assigned to them using MediLinker were calculated for each sprint. Table 3 presents these results for each sprint as well for the combined study by each week of testing. Most errors appeared to take place in entering profile information.

A majority of errors throughout this study were due to user error (formatting errors, misspelling, data not shared, etc.) Generally, the number of errors decreased with time.

### Comparison of sprint 1 and sprint 2

After completion of the 2 sprints, results demonstrate in-person clinics had higher error rates when compared with virtual clinics. MediLinker handled the transition from an in-person clinic visit to a virtual visit adequately, allowing participants in sprint 2 to easily visit online clinic sites while using the system.

As shown in Table 4, a majority of errors in sprint 1 came from formatting errors, classified as errors when inputting information into the system (spacing, capitalization, etc.). During sprint 2, data being shared with the wrong clinic was much less likely than in sprint 1 ($P < 0.05$). Incorrect data entry, defined as participants inputting data in the incorrect location within the MediLinker system, was more likely in sprint 2 when compared with sprint 1 ($P < 0.05$).

Overall, nearly half (46%) of participants accurately entered their information during all encounters in sprint 1 compared with 14% of participants in sprint 2.

MediLinker was able to manage a clinical workflow for the participants and their various avatars throughout sprint 1 and 2. Most errors occurred during data entry and verification which were categorized as human error rather than an error with MediLinker.

**Table 2.** Core principles testing identity management of MediLinker

| Principle | Testing | Results |
|---|---|---|
| Autonomy | Were participants able to own and maintain their identity independent of the identity provider? | 100% of participants were able to store their identity data on personal devices using the blockchain wallet via the MediLinker App. |
| Authority | Were participants able to control their data and EHR accounts without compromise throughout the study? | 93% of people had full control of their data and their EHR accounts were not compromised throughout the study. |
| Approval | Were participants able to voluntarily approve requests for use of their private identity? | 100% of participants were able to approve information prior to having their account accessed. One patient was able to approve login to their account on behalf of a trusted third party. |
| Confidentiality | Were participants able to successfully share and unshare their personal identifying information and healthcare data at will? | 100% subjects were able to revoke previously shared information, share/unshare information, and one subject was able to share their account details with another subject. |
| Interoperability | Were participants able to freely visit any new clinic without having to reverify their accounts? | 100% participants were able to share their avatar's data across 3 or more unconnected clinics throughout the study, indicating MediLinker has patient-centric interoperability. |
| Availability | Were participants able to access their data at any time throughout the study? | 100% of participants were able to access their data using the blockchain wallet on the MediLinker app. |

**Table 3.** Breakdown of user errors by sprint

| | Percentage of patients with errors by module and event—# participants (%age) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Weekly event | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Sprint 1 ($n = 15$) | | | | | | | | |
| Profile | 7 (46%) | 7 (46%) | 6 (40%) | 5 (33%) | 5 (33%) | 5 (33%) | 4 (26%) | 4 (26%) |
| Insurance | 14 (93%) | 13 (86%) | 11 (73%) | 13 (86%) | 12 (80%) | 11 (73%) | 11 (73%) | 11 (73%) |
| Medical | 13 (86%) | 14 (93%) | 11 (73%) | 14 (93%) | 14 (93%) | 14 (93%) | 14 (93%) | 14 (93%) |
| Credit card | 14 (93%) | 14 (93%) | 11 (73%) | 13 (86%) | 12 (80%) | 12 (80%) | 12 (80%) | 12 (80%) |
| Sprint 2 ($n = 14$) | | | | | | | | |
| Profile | 2 (14%) | 3 (21%) | 3 (21%) | 3 (21%) | 2 (14%) | 2 (14%) | 1 (7%) | 2 (14%) |
| Insurance | 12 (85%) | 12 (85%) | 10 (71%) | 11 (78%) | 10 (71%) | 9 (64%) | 9 (64%) | 9 (64%) |
| Medical | 13 (92%) | 13 (92%) | 12 (85%) | 12 (85%) | 11 (78%) | 11 (78%) | 11 (78%) | 11 (78%) |
| Credit card | 11 (78%) | 11 (78%) | 11 (78%) | 10 (71%) | 10 (71%) | 10 (71%) | 10 (71%) | 10 (71%) |
| Combined ($n = 29$) | | | | | | | | |
| Profile | 9 (31%) | 10 (34%) | 9 (31%) | 8 (27%) | 7 (24%) | 7 (24%) | 5 (17%) | 6 (20%) |
| Insurance | 26 (89%) | 25 (86%) | 21 (72%) | 24 (82%) | 22 (75%) | 20 (68%) | 20 (68%) | 20 (68%) |
| Medical | 26 (89%) | 27 (93%) | 23 (79%) | 26 (89%) | 25 (86%) | 25 (86%) | 25 (86%) | 25 (86%) |
| Credit card | 25 (86%) | 25 (86%) | 22 (75%) | 23 (79%) | 22 (75%) | 22 (75%) | 22 (75%) | 22 (75%) |

**Table 4.** Error rates of data sharing are higher for in-person clinics than virtual

| | Sprint 1 ($n = 88$) | Sprint 2 ($n = 95$) | Combined ($n = 183$) | **Significance of Difference ($P < 0.05$)** |
|---|---|---|---|---|
| Formatting errors | 47 (54%) | 43 (45%) | 90 (49%) | 0.23 |
| Misspelling | 10 (11%) | 15 (16%) | 25 (14%) | 0.33 |
| Data shared with wrong clinic | 8 (9%) | 0 (0%) | 8 (4%) | 0.003 |
| Data not shared | 14 (16%) | 12 (13%) | 26 (14%) | 0.57 |
| Incorrect data entry | 9 (10%) | 25 (26%) | 34 (19%) | 0.0053 |

## DISCUSSION

This study tested a blockchain-based, user-centric identity, and consent management application called MediLinker. While using fake patient profiles and simulated clinical and research encounters, we were able to measure the usability, functional capabilities, and potential real-world application of Medlinker. Our results show that study participants were able to use the MediLinker system to prove their identity, provide consent for data sharing, and make changes to both features during the course of the testing.

We measured the user-centric aspect of MediLinker by testing it against the 7 criteria developed by Bouras. The system was able to fulfill all testable criteria easily except for tenacity that could not be tested during the short period of our study. Participants were able to control their medical data with the share and revoke features present in MediLinker, decide which specific data elements from their profile they wanted to share with different providers, and make changes to the information in their profiles, such as change of address or a married name. All 29 participants were able to share their avatar's data across 3 or more institutions, indicating MediLinker has patient-centric interoperability.

Study results also highlighted features in the MediLinker system that needed improvement going forward. For instance, some partici-

pants unintentionally shared their data with the wrong clinic. Incorrect data entries due to user error were also observed. There were some features of the system which were not user-friendly, such as users had to delete their profile and re-enter data if they wanted to make any changes in their profile information. These features will need to be fixed in the next phase of development so that some of these fields are self-populated electronically, such as auto-pairing with the clinic the patient is visiting to avoid the patient having to choose the clinic. Similarly, the study identified shortcomings that require revamping the user interface of the system to minimize repeated data entry, erroneous formatting for addresses, dates, etc., and introducing user tips in the design of the application to assist new users with various features of MediLinker.

### Clinical Relevance

With the advent of more personalized medical diagnostic tools like molecular genetics, patients demand a more personalized user experience that combines a multitude of data sources (15). This aspect is challenged by current lack of security and the large number of hospital systems a patient interacts with, leading to a scattered trail of patient data (16). In this study, the principles of autonomy, authority, and approvability were displayed through MediLinker. These principles allow users to maintain control over their own data separately from a centralized source and make independent decisions without influence from untrusted third parties. Patients should be able to easily access their data at any time and decide who it is shared with. Enabling patients' control over when their records are shared and with whom, would allow for a more effective sharing of data among providers.

Patients' ability to share their own data with multiple providers may significantly address the inefficiencies and lack of care coordination created by fragmented and siloed EHR systems of today (17). Despite significant investments in promoting interoperability, its impact on improved patient satisfaction or provider coordination has not been remarkable (18). At the same time, security and privacy concerns about legacy information systems and centralized electronic databases maintained by providers still persist (19, 20). As shown in this study, fulfilling the principle of interoperability using blockchain technology can help overcome some of these challenges effectively. Interoperability of medical records is an important component of a patient-centric healthcare system (1), and not only reduces provider burden to piece together information from multiple sources but also gives patients the control and autonomy to select their providers and actively participate in their own care. Patient-mediated information exchange also helps in ensuring accuracy and update of data related to the patient.

The principles of confidentiality and interoperability enable patients to share their account details with a caregiver, if needed to pick up medications or assist with medical visits. A feature allowing for other users to access one's health account is paramount especially during times of crisis, when some demographics are more susceptible than others. This can be seen during the COVID crisis where an older demographic is more at risk, but still may need medications that need to be picked up from a pharmacy. Allowing a trusted third party to access their account would overcome this problem, while still maintaining confidentiality for the individual user (21).

### Study limitations

The study used students to act as patients with varying ages and experiences. Ethnicity, age, or other patient characteristics were randomly assigned to study participants without trying to match anyone to a certain avatar. Not having actual patients limited our understanding of how an actual person might use the system but as a pilot test for a blockchain application, we did not consider the additional insights gained to be worth the risk of using real patients or their data. We also tested a limited number of use cases and scenarios which can be further expanded in future research.

### Future Research

Our study provides preliminary evidence of the feasibility of using a blockchain-based patient-centric identity management system for patients. We identified several design features in the system that may be improved to ensure improved usability, error avoidance, and security. While we tested the system in different simulated clinical and research environments using various patient profiles, there is a need to further test the identity transactions for more complex use cases, such as those with mental disorders, incarcerated, or nonEnglish speakers. The sudden changes in research and social environments due to COVID-19 pandemic allowed us to demonstrate the application of the identity management system for virtual visits but it does create more challenges to verification of documents that can be done during an in-person visit. More research is needed to test the various biometric and zero knowledge identity options to make the system ready for real-world applications. There are social, ethical, and behavioral aspects of the study that can be further explored. For instance, how a system like this may be perceived by different groups based on their age, ethnicity, or familiarity with technology. Similarly, further research is needed to understand adoption by healthcare providers and other public and private stakeholders who need identity verification to deliver their services and fulfill regulatory and legal requirements. Adoption by different patient groups will also need to be studied further by testing actual patients' usability and perceptions of using identity management systems that are based on different methods including applications like Medilinker for health information exchange (22).

## CONCLUSION

Blockchain technology holds great promise in developing patient-centric identity management systems as demonstrated by our MediLinker study. MediLinker successfully fulfilled the criteria delineated by Bouras for user-centric identity management systems. MediLinker helped patients control their own information, decide what to share with whom, and facilitated identity verification. It also allowed patient-mediated interoperability and data sharing among various clinics in a secure and auditable manner. The study also identified usability features that can be further improved and pointed to future research for continued development of these ideas while ensuring human subjects protection.

## FUNDING

This work was partially supported by the University of Texas Blockchain Initiative and the Dell Medical School at the University of Texas at Austin.

## AUTHOR CONTRIBUTIONS

All authors (AK, CH, CC, JA, DTH, MU, ID, JRB, EM) were involved in the design, acquisition of data and its interpretation, drafting/revising the manuscript, and for final approval of the original and revised manuscripts. All authors also agree to be accountable for the accuracy and integrity of the work presented here.

## ACKNOWLEDGMENTS

The authors would like to thank the University of Texas Blockchain Initiative for providing partial funding for this work. Bullard Research Fellowship of the School of Information supports Dr Bautista as a postdoctoral research fellow. They would also like to thank the students who participated in the study and our project team members including Ladd Hanson, Prof. Sarfraz Khurshid, Eliel Oliveira, and Jahnavi Shriram.

## CONFLICT OF INTEREST STATEMENT

The authors have no competing interest to declare.

## DATA AVAILABILITY

The data underlying this article will be shared on reasonable request to the corresponding author.

## REFERENCES

1. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Comput Struct Biotechnol J* 2018; 16: 224–30.
2. Kuo T-T, Hsu CN, ModelChain Ohno-Machado L. Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. Gaithersburg, MD: ONC/NIST Use of Blockchain for Healthcare and Research Workshop; 2016.
3. Azaria A, Ekblaw A, Vieira T, *et al*. Medrec: using blockchain for medical data access and permission management. In: *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE; 2016; 25–30.
4. Voigt P, Von Dem Bussche A. The eu general data protection regulation (gdpr). *A Practical Guide, 1st ed. Cham (Switzerland): Springer International Publishing*; 2017.
5. Evans R. Electronic health records: then, now, and in the future. *Yearb Med Inform* 2016; 25 (Suppl 01): S48–61.
6. Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. *J Am Med Inform Assoc* 2017; 24 (6): 1211–20.
7. Greenspan G. Multichain private blockchain-white paper. 2015. http://www.multichain.com/download/MultiChain-White-Paper.pdf. Accessed January 11, 2011.
8. Ivan D. Moving toward a blockchain-based method for the secure storage of patient records. 2016. https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf. Accessed August 14, 2020.
9. Brodersen C, Kalis B, Leong C, *et al*. Blockchain: securing a new health interoperability experience. *Accenture LLP*. 2016; 1–11.
10. Justinia T. Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. *Acta Inform Med* 2019; 27 (4): 284.
11. Khurshid A, Gadnis A. Using blockchain to create transaction identity for persons experiencing homelessness in America: policy proposal. *JMIR Res Protoc* 2019; 8 (3): e10654.
12. Baer N. First, do no harm. *J Clin Ethics* 2013; 24 (1): 64–6.
13. Pubmed Search Results. https://pubmed.ncbi.nlm.nih.gov/?term=blockchain+and+Healthcare&filter=years.2016-2017. Accessed October 18, 2020.
14. Bouras MA, Lu Q, Zhang F, *et al*. Distributed ledger technology for eHealth identity privacy: state of the art and future perspective. *Sensors* 2020; 20 (2): 483.
15. Dudley JT, Listgarten J, Stegle O, Brenner SE, Parts L. Personalized medicine: from genotypes, molecular phenotypes and the quantified self, towards improved medicine. *Pac Symp Biocomput* 2015: 342–6.
16. Meingast M, Roosta T, Sastry S. Security and privacy issues with health care information technology. *Conf Proc IEEE Eng Med Biol Soc* 2006; 2006: 5453–8.
17. Burton LC, Anderson GF, Kues IW. Using electronic health records to help coordinate care. *Milbank Q* 2004; 82 (3): 457–81.
18. Gold M, McLaughlin C. Assessing HITECH implementation and lessons: 5 years later. *Milbank Q* 2016; 94 (3): 654–87.
19. Fernández-Alemán JL, Señor IC, Lozoya PÁ, *et al*. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform* 2013; 46 (3): 541–62.
20. Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States [published correction appears in JAMA. 2015 Jun 23–30;313(24):2497]. *JAMA* 2015; 313 (14): 1471–3.
21. Mayer AH, da Costa CA, Righi RdR. Electronic health records in a Blockchain: a systematic review. *Health Inform J* 2020; 26 (2): 1273–88. Published online1460458219866350.
22. Esmaeilzadeh P, Mirzaei T. The potential of blockchain technology for health information exchange: experimental study from patients' perspectives. *J Med Internet Res* 2019; 21 (6): e14184.