BLOCKCHAIN™ IN HEALTHCARE TODAY

ORIGINAL RESEARCH

Technical Design and Development of a Self-Sovereign Identity Management Platform for Patient-Centric Health Care using Blockchain Technology

Daniel Toshio Harrell, PhD[1]; Muhammad Usman, MS[2]; Ladd Hanson, BA[3]; Mustafa Abdul-Moheeth, MD[1]; Ishav Desai, BS[1]; Jahnavi Shriram, BS, BA[1,4]; Eliel de Oliveira, MS, MBA[1]; John Robert Bautista, RN, MPH, PhD[5]; Eric T. Meyer, PhD[5] and Anjum Khurshid, MD, PhD[1]

[1]University of Texas at Austin-Dell Medical School, USA; [2]University of Texas at Austin-Department of Electrical and Computer Engineering, USA; [3]University of Texas at Austin-Information Technology Services, USA; [4]University of Arizona College of Medicine- Phoenix, USA; [5]University of Texas at Austin-School of Information, USA

Corresponding Author: Anjum Khurshid, Email: anjum.khurshid@austin.utexas.edu

Keywords: blockchain technology, decentralized identifiers, health information, hyperledger, self-sovereign identity, verifiable credentials

Abstract

Objective: Clinical data in the United States are highly fragmented, stored in numerous different databases, and are defined by service providers or clinical specialties rather than by individuals or their families. As a result, linking or aggregating a complete record for a patient is a major technological, legal, and operational challenge. One of the factors that has made clinical data integration so difficult to achieve is the lack of a universal ID for everyone. This leads to other related problems of having to prove identity at each interaction with the health system and repeatedly providing basic information on demographics, insurance, payment, and medical conditions. Traditional solutions that require complex governance, expensive technology, and risks to privacy and security of the data have failed adequately to solve this interoperability problem. We describe the technical design decisions of a patient-centric decentralized health identity management system using the blockchain technology, called MediLinker, to address some of these challenges.

Design: Our multidisciplinary research group developed and implemented an identity wallet, which uses the blockchain technology to manage verifiable credentials issued by healthcare clinics, banks, and insurance companies. To manage patient's self-sovereign identity, we leveraged the Hyperledger Indy blockchain framework to store patient's decentralized identifiers (DIDs) and the schemas or format for each credential type. In contrast, the credentials containing patient data are stored 'off-ledger' in each person's wallet and accessible via a computer or smartphone. We used Hyperledger Aries as a middleware layer (API: Application Programming Interface) to connect Hyperledger Indy with the front-end, which was developed using a JavaScript framework, ReactJS (Web Application) and React Native (iOS Application).

Results: MediLinker allows users to store their personal data on digital wallets, which they control. It uses a decentralized trusted identity using Hyperledger Indy and Hyperledger Aries. Patients use MediLinker to register and share their information securely and in a trusted system with healthcare and other service providers. Each MediLinker wallet can have six credential types: health ID with patient demographics, insurance, medication list including COVID-19 vaccination status, credit card, medical power of attorney (MPOA) for guardians of pediatric or geriatric patients, and research consent. The system allows for in-person and remote granting and revoking of such permissions for care, research, or other purposes without repeatedly requiring physical identity documents or enrollment information.

Conclusion: We successfully developed and tested a blockchain-based technical architecture, described in this article, as an identity management system that may be operationalized and scaled for future implementation to improve patient experience and control over their personal information.

Received: December 1, 2021; Revised: January 6, 2022; Accepted: January 6, 2022; Published: March 18, 2022

The 21st Century Cures Act (Cures Act), signed into law in 2016, has made it mandatory for the federal government to find ways of accessing patient data faster and more efficient.[1] Billions of dollars have been spent by the Government of United States to promote and improve the electronic medical record (EMR) systems in its healthcare system. Unfortunately, the fragmented design of the health system and lack of a universal unique identity (ID) number for everyone have created a highly siloed data ecosystem for medical records. As a result, a patient must prove his or her identity to each provider individually, and during every clinical visit, he or she must fill out forms and provide additional, usually repetitive, information. Without identity verification, providers may refuse services, or be unable to read and write health information within the patient's data stream. There is no reliable method for patients to give, reference, and revoke consent for providers to access their health information.[2] Consent to read, write, and share health information is often obtained by the patient signing a paper form, which makes accessing and revoking consent impractical or impossible for most patients.

A blockchain is a digital ledger of transactions distributed across a trusted peer-to-peer network of nodes, and was first implemented to allow exchange of cryptocurrencies such as bitcoin and other financial transactions.[3] Beyond blockchain's original financial use cases, researchers[4–7] have suggested that blockchain technology's distributive model can bridge the gap between the "data silos" in health care and may improve coordination between healthcare providers and patients.[5,8,9] This empowering and potentially disruptive technology can provide a novel data model, which provides patients control over their medical data. Besides, blockchain implementations have been proposed for other healthcare use cases, such as improving the management of research consent,[10] clinical trials,[11,12] supply chains,[13] and healthcare provider's accreditations.[14]

Background

Currently, there is a limited understanding about the technical design and development of a reliable patient-centric healthcare identity platform using blockchain technology for navigating and resolving a fragmented healthcare data environment. In this article, we describe the technical design and development of our blockchain solution, MediLinker, which has been tested in simulated real-world settings.[15] MediLinker provides patients with a digital healthcare identification method and control over how their medical data are stored, shared, and accessed.

Methods

Use-case Designs for MediLinker

Our MediLinker system design is guided by clinical use cases as specified by medical providers and residents at Dell Seton Medical Center in The University of Texas (Austin, Texas).

With MediLinker, users can complete the following seven use cases:

1. Initial enrollment at first clinic and creating validated credentials,
2. Enrollment at second clinic with only validated digital credentials,
3. Presenting or consenting personal or medical data with clinics,
4. Patient changing personal information on Blockchain wallet and validating the modification,
5. Patient consent to participate in research projects,
6. Patient removing full or partial consent with clinics with credential revocation,
7. Medical Power of Attorney (MPOA)/Digital guardianship for geriatric and pediatric patients.

We initially tested the MediLinker system for enrolling patients, presenting demographic or medical information to multiple clinics, editing their demographic information, consenting to participate in research projects, and revoking credentials.[15] Later, we added the issuance of a MPOA/Guardianship for the agents of geriatric and pediatric patients. For MPOA design, we relied on the Texas Health & Human Services Commission Medical Power of Attorney Designation of Health Care Agent form.[16] With MediLinker, participants can manage and present credentials using their family members' MediLinker accounts from their device.

MediLinker also enables patients to revoke already credentialed data shared among the clinics and institutions within the network of trust. Only the issuer of a credential, such as a government agency, can revoke credentials upon request from the credential holder. While revocation does not delete data from an institution, the patient's desire to deny future usage is recorded on the blockchain and the data set is no longer verifiable in future shares.

Blockchain Frameworks

For our healthcare identity management use cases, we required a blockchain framework that can issue patient-held verifiable credentials and then share them securely with multiple institutions. We conducted a detailed environmental scan of existing and proposed blockchain solutions that could provide the appropriate technical platform for an identity management system. This process involved search in electronic databases, discussion with key informants, and review of news and blogs in blockchain-focused online resources.

We selected and reviewed in detail the following two potential blockchain frameworks for the development of our identity management system:

Citation: Blockchain in Healthcare Today 2022, **5**: 196 - http://dx.doi.org/10.30953/bhty.v5.196

- Ethereum: It is an open-source platform that uses a proof-of-work algorithm and ensures immutability. Smart contracts allow credible transactions to take place without the presence of third parties. This allows interoperability between physicians, patients, and other third parties. However, the focus of Ethereum is on transactions and smart contracts rather than identity management.[17]
- Hyperledger Indy: It is founded by Sovrin Foundation in 2018.[18–20] It is a platform specifically designed for identity management with a focus on self-sovereign identity (21). Users have full autonomy over their information and decide who gets access to which part of their data. It uses a decentralized ledger with a registry of decentralized identifiers (DIDs). It is used for retrieving and storing public DIDs for pairwise communication, which increases the security and privacy of identity.[20,22]

Front-end Frameworks, Cloud Service Providers, and Authentication

There are many popular front-end frameworks that can be used to develop web and mobile applications. While blockchain frameworks provide the required functionality at the back-end, user interaction with the system needs to be facilitated using front-end applications. For web applications, some of the commonly used solutions include VueJS, AngularJS, and ReactJS. Kotlin can be used to develop Android applications, and Swift can be used to develop iOS applications. Another option is to use the React Native framework to develop both Android and iOS applications using the same code base.

The MediLinker application controls software running on a virtual machine (VM) in the cloud called a digital agent. The agent software takes actions on behalf of the patient like accepting connection requests and managing communications with other digital agents. Servers are also required to store patient's and clinic's agents. Cloud services can be used to create VMs that can store these agents. The advantage of cloud service is that it is more scalable. There are three main global cloud providers which include Google Cloud Platform, Microsoft Azure, and Amazon Web Services (AWS). For authentication, the patients can use their login credentials (i.e. username and password) to login into the application. Two-factor authentication and biometric authentication are also among the possible options.

Team Design

To develop our healthcare-related blockchain solution, we formed an interdisciplinary collaboration, including medical and design researchers, blockchain subject-matter experts, developers, software engineers, and social scientists. Throughout the development, physicians, medical residents, and students helped in defining the patient journey in the clinical workflow. This team also helped develop patient profiles, the most common clinical scenarios, and information needed for testing the functionality of the final product in a simulated environment.

Development Phases

MediLinker was developed over the period of 2 years (2019–2021). The timeline was divided into two phases: phase 1 (2019–2020) and phase 2 (2020–2021). During phase 1, we developed a web application with the basic use cases. During the development of phase 1, Hyperledger Aries did not support the revocation of credentials. Therefore, patients could not revoke data from the web application. However, the revocation feature became available from Hyperledger Aries during phase 2 development. We plan to add the revocation feature in the web application as part of future work.

In the second phase, we developed a more robust iOS/Android application and expanded our use cases to include legal guardianship of minors and geriatric patients. With the MediLinker iOS/Android application, users can present and revoke patient-controlled data from a patient's phone, while improving system access with on-device biometric authentication. Participants with MPOA can act on behalf of their family members through the application. This allows users to issue and share credentials as their family members' MediLinker accounts from their device. Users can also revoke previously issued credentials, by which patients can stop future verifications of their data.

Results

Six MediLinker Verifiable Credentials: Health ID, Insurance, Medications, Credit card, Research Consent, and MPOA

MediLinker is a digital wallet with six verifiable credential types: health ID, insurance, medications, credit card, research consent, and MPOA (Figure 1a). The data fields in MediLinker are provided in Table 1. These credential types were chosen based on our clinical team's experience of the minimum requirements of information needed during clinical encounter. The Health ID credential includes demographic information about the patient based on a government-issued ID and their contact information. The insurance credential stores information about a patient's health insurance as specified on a patient's insurance card. The medication's credential includes information about patient's medication, dosage, and COVID-19 vaccination status. The credit card credential stores billing information about a patient. The research consent credential includes information about the research study and the record of the patient's consent participation in the study. The MPOA credential includes information about the guardians and their dependent.

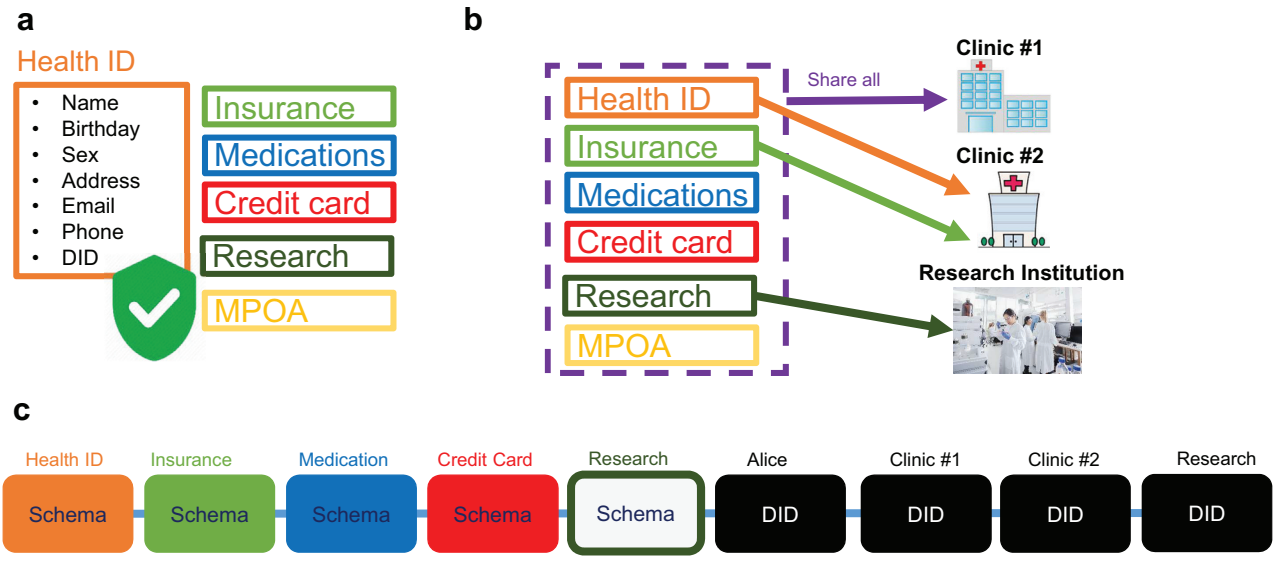

Fig. 1. MediLinker credentials and blockchain design. a) MediLinker account consists of six verifiable credentials: health ID, insurance, medications, credit card, research consent, and Medical Power of Attorney (MPOA). b) A patient can share all or a desired subset of verified information to multiple institutions. c) The blockchain includes the schemas of each credential type and decentralized identifiers (DIDs) of patients and institutions.

Once these credentials are verified, a patient can share all or a subset of his or her information across multiple, preferred healthcare providers (Figure 1b), providing patients autonomy and interoperability between clinics. While the patient information is stored securely within the digital wallet, only the schemas of each credential type and DIDs of each patient and healthcare institution are available on the blockchain, thus ensuring security and privacy of the data while allowing the transactions to occur seamlessly (Figure 1c). Patients can always see which data are shared with each institution.

MediLinker Clinical and Credentialing Workflows

MediLinker enables the issuing and holding of verifiable credentials in their wallet for each type, which are issued by an "Issuer" and held by a "Holder." With exception of the research consent credential, an institution's representative, such as a clinic receptionist or registration clerk, "issues the MediLinker credentials after review by the patient." In contrast, research consent credentials are issued and reviewed by the research participant, and then held by the institution. The patients hold the issued verified credential in their digital wallet.

The credentialing workflow relies on a government-issued identity or third-party paper-based credentials to be digitized, stored, and shared securely through the blockchain. Using MediLinker, patients can establish a connection between them and a trusted institution by scanning the QR Code available at the clinic. Using the web application, the patient enters his or her medical data and then presents his or her government-issued identity or other physical cards to a receptionist for verification (Figure 2a). For iOS application, a receptionist enters the data to create the patient's verifiable credentials based on physical cards, which are then reviewed and approved by the patient (Figure 2b). This change in workflow was implemented to avoid data entry errors by patients,[15] and the inclusion of revocation into the Hyperledger framework by an issuer. Once approved, the receptionist can issue the credential to the patient's wallet, which is verified and sharable digitally with participating institutions without the need for showing physical documentation (Figure 2c). The same workflow is used for creating verifiable credentials for credit card from a bank and insurance cards from an insurance company.

The research consent credential is created by the participant, reviewed by research institution, and then issued by the participant. With the participant as the "Issuer," they can revoke the credential without the need for asking the research institution.

The MPOA credential and workflow enable geriatric or pediatric patient's family member to create and edit credentials on their behalf through the application. A geriatric or pediatric patient in their MediLinker account asks a notary organization to create and issue a MPOA credential. Once shared with the guardian's MediLinker account, the guardian can switch between his or her account and his or her dependent's accounts, by which the guardians are able to share their family member's data from their own account. We also developed a notification

Citation: Blockchain in Healthcare Today 2022, **5**: 196 - http://dx.doi.org/10.30953/bhty.v5.196

Table 1. Data fields in each MediLinker credential: health ID, medications, insurance, credit card, research consent, and MPOA

Credential	Data fields
Health ID	Given name
	Surname
	Street address
	City
	State
	Zip code
	Country
	Sex
	Gender
	Date of birth
	Email
	Phone number
Medications	Medications
	Dosage
	COVID-19 vaccination status
Insurance card	Patient's name
	Plan
	Group
	Provider's name
	Member ID
	Emergency-room charge ($)
	Deductible ($)
	Co-pay ($)
	Expiry date
Credit card	Patient's name
	Credit card number
	Expiry date
Research consent	Research study name
	Participant's consent
MPOA	Guardian's given name
	Guardian's surname
	Guardian's address
	Guardian's phone number
	Dependent's given name
	Dependent's surname
	Dependent's address
	Dependent's phone number

system to improve alertness of actions within MediLinker. If a participant or institution shared or revoked a credential, the holder of the credential is alerted with a banner notification.

MediLinker was designed for in-person interactions before the COVID-19 pandemic. However, due to COVID-19 lockdowns in the United States, we were able to test our system in a virtual clinic environment without any additional technical development. After clinical workflow modifications to virtual sessions, participants were able to seamlessly use the system's features and complete the same clinical scenarios in a virtual clinical setting over Zoom (Zoom Video Communications, San Jose, CA).[15] As discussed below, these seamless practical and workflow adjustments indicated system's applicability for telemedicine, virtual care, and other home care settings.

MediLinker Technical Framework

Blockchain Framework – Hyperledger Indy

Based on the methods described above, where we evaluated two platforms and examples of previously developed blockchain-based identity systems, we selected Hyperledger Indy[20,22] to develop MediLinker. The decision was influenced by Hyperledger Indy's characteristic of a decentralized identity framework, which best aligns with patient's information protection and full autonomy over his or her data. Hyperledger Indy was used to store data schemas and credential definitions for provider–patient relationships based on the concept of decentralized trusted identity.[12] DIDs are a World Wide Web Consortium (W3C) specification that allows for a verifiable, decentralized digital identity.[20,23] This allows the controller of DID (e.g. the patient) to prove his or her identity without a centralized registry or identity provider, and without requiring permission from a third party. Hyperledger Indy makes the creation and use of DIDs convenient on its platform.

Besides adopting Hyperledger Indy for MediLinker, we adopted Hyperledger Aries to act as a middleware layer (API) to connect Hyperledger Indy with the front-end. Hyperledger Aries implements a RESTful programming interface to handle different workflows and interactions, which helps in creating, transmitting, and storing verifiable digital credentials efficiently.

The development of MediLinker showed that the design of Hyperledger Indy and Hyperledger Aries allows those with no prior experience of blockchain application development to use these platforms. The auto-acceptance of credentials built into Hyperledger Indy makes it extremely useful to experiment with the frameworks. Once the developers get experience in using the framework, automated acceptance and rejection of credentials can be replaced with programming code.

Front-end Framework—ReactJS and React Native

The front-end of web application was developed using a JavaScript framework, React JS (Facebook Open Source, Menlo Park, CA).[24,25] It allows developers to break down the user interface into multiple components making the programming of web applications much simpler. React JS also uses a "Virtual Document Object Model" that can detect which components have changed so that only the required components are rendered. This results in a faster application with a better user experience (Figure 3).

We also developed mobile applications for MediLinker to make it accessible from mobile devices. We used the

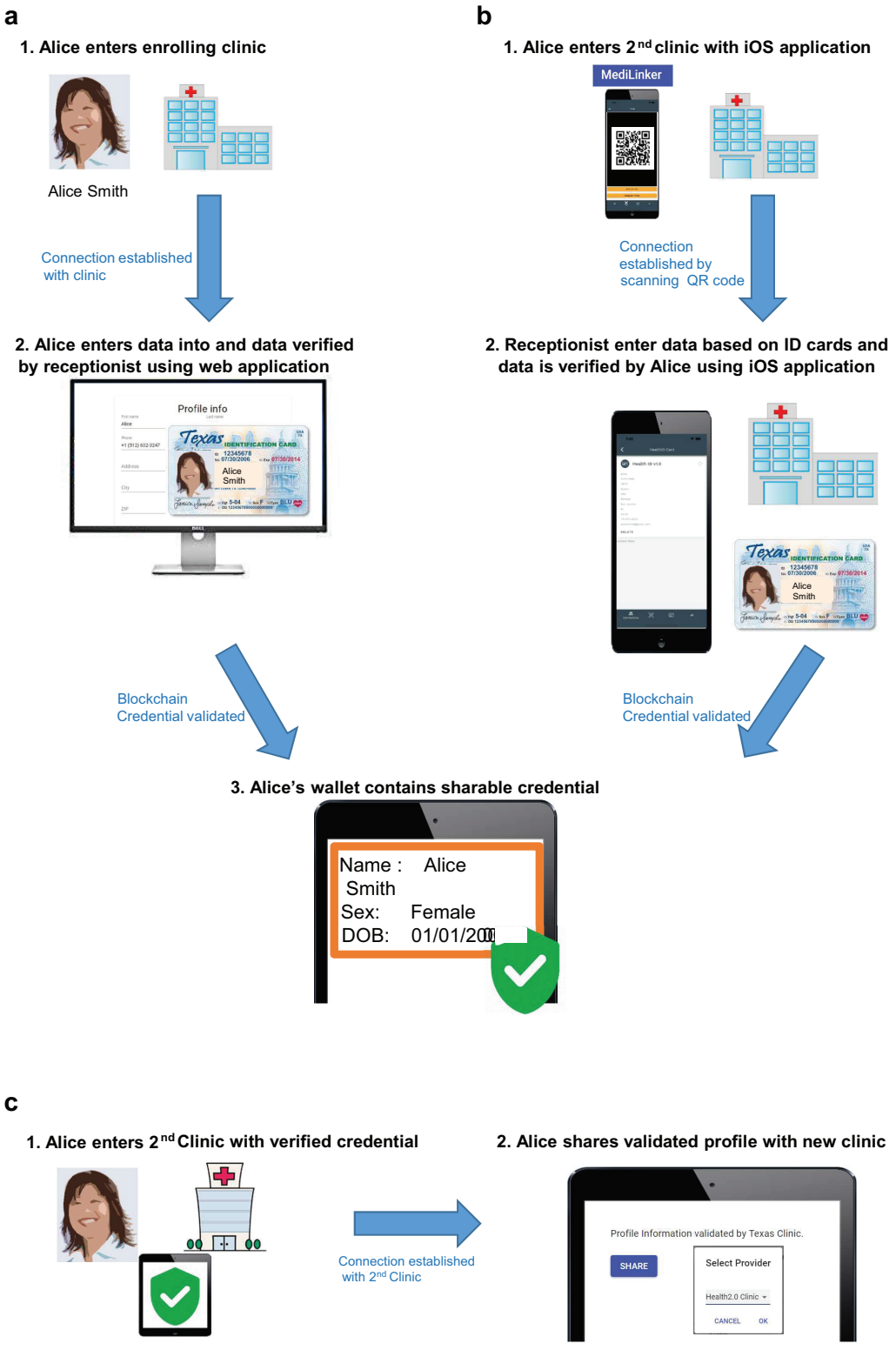

Fig. 2. MediLinker clinical workflows and two-way verification process. a) A patient, Alice, enrolls at a new clinic, and enters her information into MediLinker application with a web application. Once submitted, a receptionist verifies her data against information available on a verified card such as a government-issued ID. b) With MediLinker iOS application, the receptionist enters data based on the presented government-issued ID, which is reviewed and verified by the patient. Once verified by both patients and receptionist, a validated blockchain credential is issued, which is useable in other participating clinics. c) At a second clinic, Alice can share her digitized verified healthcare information through MediLinker web/mobile application.

Citation: Blockchain in Healthcare Today 2022, **5**: 196 - http://dx.doi.org/10.30953/bhty.v5.196

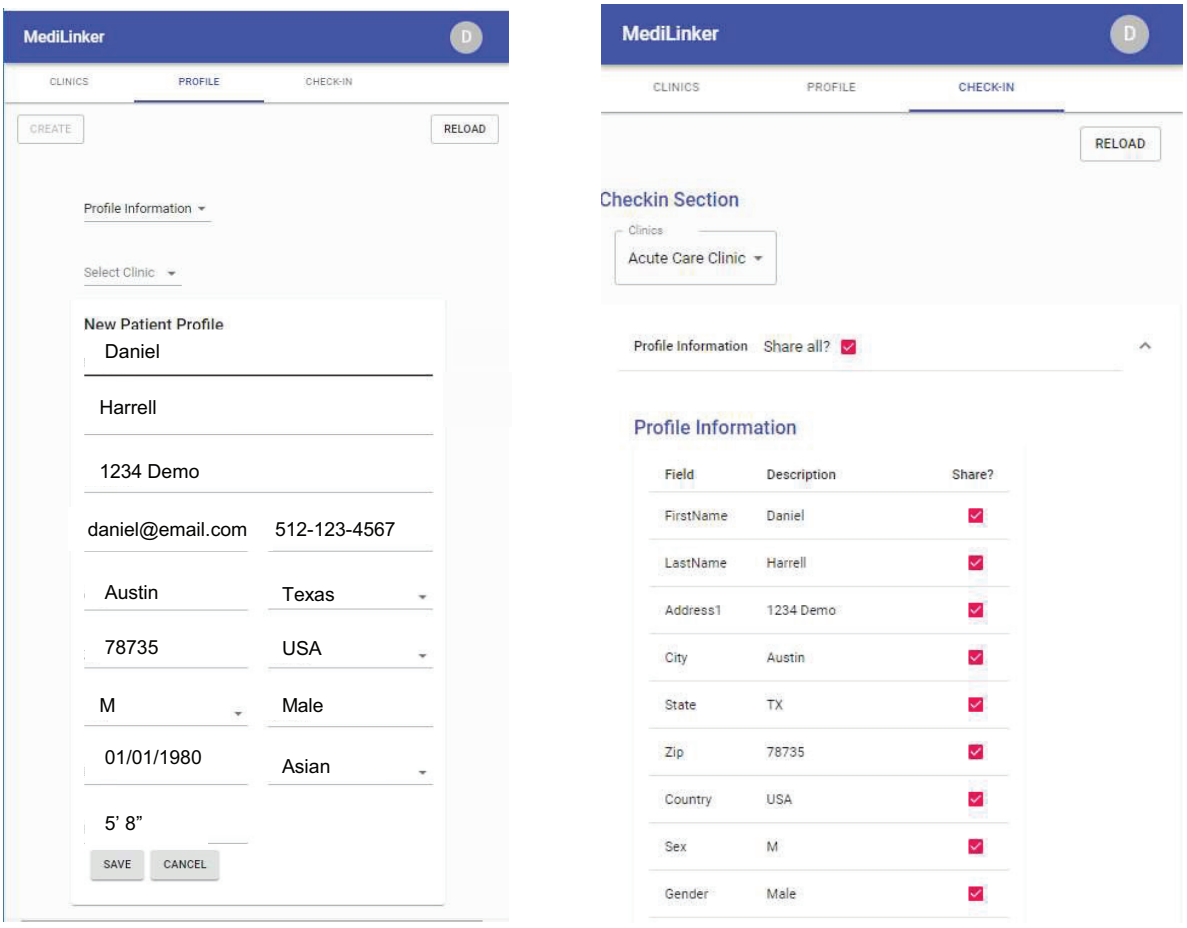

Fig. 3. MediLinker web application UI (user interface). MediLinker is a web application by which patients and receptionist can interact with their MediLinker agent. The web application was developed in React JS.

React Native framework (Facebook Open Source, Menlo Park, CA)[26] to implement native mobile applications (Android/iOS) using the same code base (Figure 4). This allows patients to have a more interactive experience via their mobile phones. We used the Material-UI (Material-UI [user interface] SAS, Paris, France) framework for implementing UI components.[27]

Cloud Service Provider – Amazon Web Services

We expect that MediLinker would work on any public cloud without much modification; however, we used AWS (Amazon Web Services, Inc., Seattle, WA) to host Hyperledger Indy servers and Hyperledger Aries agents. The choice of the cloud service was based on convenience because the University has a campus-wide contract with AWS, so it was practical to get an account. AWS is a leading public cloud provider and is Health Insurance Portability and Accountability Act (HIPAA) compliant, which is required for future adoption in a clinical setting. A VM is required to host each patient's agent. AWS allows us to create and run VMs with a customized schedule of when the VMs should be running. This helps save cost during development because the developer can shut down the VMs when they are not needed.

Hosting VMs also allows the ability to scale the system to N patients and M clinics. In the experiments, we successfully scaled the system from 1 patient to 20 patients. This keeps each of the patients' agents separate from each other. If one server or VM is compromised, the rest of the agents are isolated and secured (Figure 5). This solution worked for our scenario because it was tested using 20 patients' agents. This technique may not be scalable in a setting where there are many patients. In such a scenario, Docker containers[28] hosted on a single VM are recommended. For the web application, no installation at clinic or patient's side is required. For the mobile application, the application was provided to study participants using the Apple TestFlight application. For adoption in a clinical setting, the application can be distributed via Google Play Store and Apple Store.

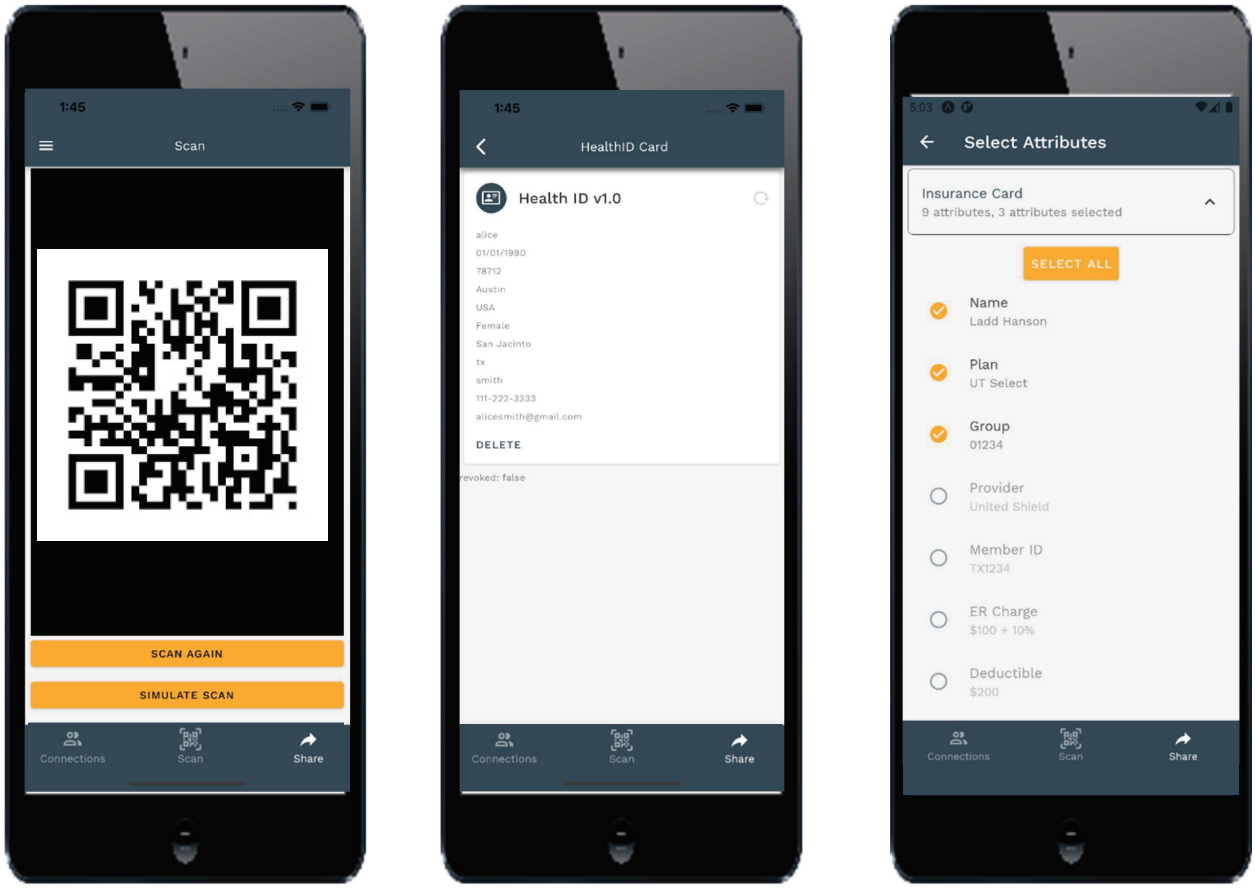

Fig. 4. MediLinker mobile iOS application UI. Patients and receptionist can also interact with their mobile devices. The MediLinker mobile application was developed in React Native, which can be used on iOS and Android devices.

Authentication

For the web application, we developed MediLinker's authentication system that requires users to enter a username and password to log into their accounts. Biometric authentication is not a feasible option for web applications because these applications are mostly accessed via personal computers, and to enable biometric authentication, patients should have a fingerprint scanner or similar devices attached to their computers, which is not common. Moreover, one of the goals of developing MediLinker was to allow people experiencing homelessness to manage their identity. It is common that many people experiencing homelessness do not have smartphones.[29, 30] For the native mobile applications, the patients are provided with the option to login using their phone's native biometric authentication (fingerprints for Android devices and TouchID/FaceID for iOS devices).

Discussion

In this article, we have described the design and development of a blockchain-based, patient-centric healthcare identity and research consent management application, MediLinker. The unique features of this system promise to add features that are lacking in current management of personal health information and might take many years to achieve. This includes interoperability among diverse information systems, patients' control over their own data, and ability to prove identity without having to carry physical evidence at each interaction within the system. Some of the following aspects are of particular importance:

MediLinker Healthcare Identity Use for Health Information Exchange

As mentioned earlier, fragmentation of clinical data and lack of interoperability among health information systems create safety concerns for patients and result in inefficiencies in the delivery of care. Health Information Exchanges (HIEs) are platforms that are developed to connect disparate health information systems and EMRs through a central hub. While HIEs may provide an alternative solution to the interoperability issue in the United States, in which patient EMRs are sharable through a centralized data repository,[31] the patient data are still controlled by the institutions rather

Citation: Blockchain in Healthcare Today 2022, **5**: 196 - http://dx.doi.org/10.30953/bhty.v5.196

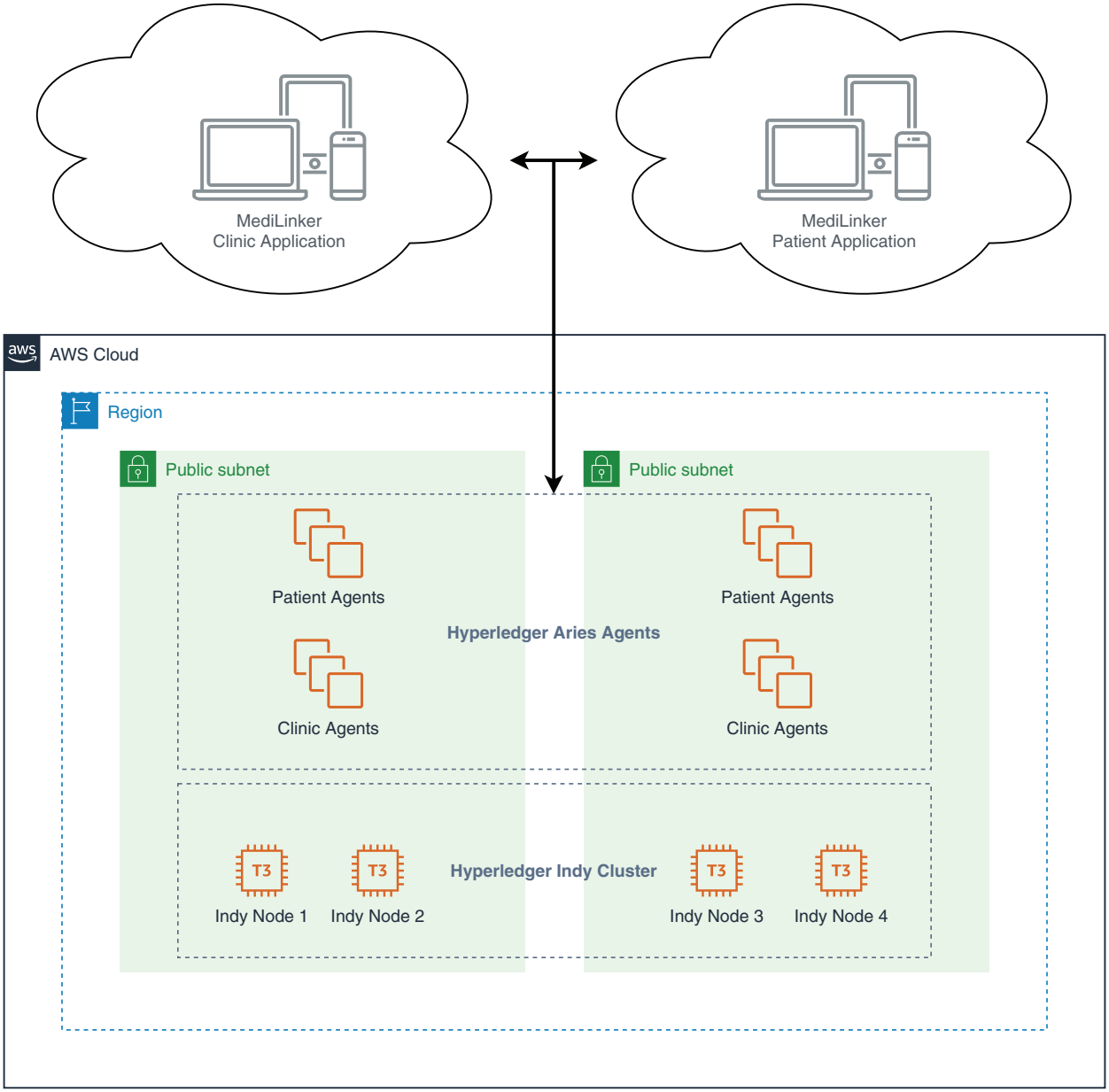

Fig. 5. MediLinker system architecture. Front-end web application is developed using ReactJS, a JavaScript framework. Front-end mobile application is developed using React Native. The back-end layer consists of a cluster of Hyperledger Indy nodes. The front-end layer is connected with the back-end layer using an intermediate layer, which consists of Hyperledger Aries agents (patients and clinics agents). A virtual machine (VM) is required to host each patient's agent. Each of the patients' agents is separate from each other. If one server or VM is compromised, the rest of the agents are isolated and secured.

than the patient.[32] A central data repository has its advantages but also provides a single point of breach or failure, thus increasing the threat to patient privacy and data security. Blockchain technologies are a decentralized alternative[9,11,33,34] that leverage their distributed architecture model towards establishing a patient-centric and patient-controlled sharing of medical records across isolated institutions preserving the continuity of care. As designed, MediLinker provides the Health ID credentialing, verification, and management to bridge a fragmented system with patients as the focus. Furthermore, the credentialed digitized MediLinker ID can provide a common patient identifier by which connections in a trust network between healthcare providers, insurance companies, and patients can be established toward minimizing patient-matching issues.

MediLinker Usage as Identity Management for Vulnerable Populations

Blockchain technologies can help create a transactional identity for vulnerable populations in need of social and health care, such as persons experiencing homelessness.[35,36] Often individuals lose or misplace their government-issued identifications and medical paperwork, which are needed to interact with social services and the medical system. Beyond MediLinker's initial objective, our users can digitize and share digital versions of patient-held ID cards. With this digitization of physical ID, MediLinker enables patient populations to hold a secure electronic health ID that is easily managed and recoverable on smartphones or computers toward improving their healthcare access.[15]

MediLinker Adaptation to Virtual Clinical Workflows and Vaccination Status Management During the COVID-19 Pandemic

Although designed for in-person clinical visits, MediLinker was also tested during COVID-19 lockdowns in the United States in 2020. The system worked successfully in virtual clinic visits, allowing patients to use the system to register and provide their information and consent. Given the need for social distancing in a COVID-19 world, the ability to share verified identifiers and medical records for a contactless and virtual format is a major advantage of using blockchain-distributed ledger systems in future clinical workflows.

Furthermore, MediLinker is designed to track patient's current medications and dose for sharing with healthcare providers. MediLinker application can be used to digitally track individual vaccination doses, as a COVID-19 passport, that is verifiable.[37] Using a zero-knowledge proof, a person's vaccination record can be shared to clinics and institutions without presenting other personal information. Furthermore, MediLinker could provide a verified and digital record of the COVID-19 Vaccination Record Card and serve as an immunity passport for future travel.

Limitation of current work and future research

The MediLinker system was developed to understand how to design and demonstrate the use of DIDs and verifiable credentials in patient identity management while allowing reasonable room for future improvements. The fields in MediLinker were free text to explore all human interactions and errors. In the future, we plan to add validation checks to fields, which will allow patients to enter data only in a specified format.

While the current implementation is approaching a minimum viable product (MVP), our team desires to transition MediLinker to an operational product in clinical settings. In the next step, we plan to integrate MediLinker with EMR systems to manage highly sensitive medical records. Furthermore, this trust network between participants and institutions must include a means of ensuring patient privacy as well as verification of the patient's presence during digital encounters, something described as a Liveness Test. We plan to continue to develop our electronic decentralized identity management system (MediLinker) toward becoming operational in a real-world healthcare setting.

Conclusions

MediLinker is a blockchain solution for identity management designed to allow patient autonomy and interoperability between clinics using a custom-built web and mobile application. The technical design and development of MediLinker show how Hyperledger Indy combined with Hyperledger Aries can be used to develop an operational identity management system for patients. It allows patients to securely log in, verify their credentials, and share those credentials from their blockchain wallets to other organizational entities on the blockchain. Our technical design allows patients to have control over their identity data by using the DIDs functionality of the underlying blockchain platform. We have shown that the technical architecture adopted for MediLinker demonstrated a proof-of-concept patient-centric identity management system that can be operationalized and scaled for future implementation in healthcare settings and provide patients the privacy and control desired for personalized health data.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

This study was partially funded by the University of Texas-Blockchain Initiative, and the authors acknowledge its support for this work. John Robert Bautista acknowledges the support of the Bullard and Boyvey Fellowship awarded to him by the School of Information, The University of Texas at Austin. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Contributors

As per the "Role of Authors and Contributors" outlined by ICMJE, each author participated in the conception or design of the work; or the acquisition, analysis, or interpretation of data for the work; AND Drafting the work or revising it critically for important intellectual content; AND Final approval of the version to be published; AND Agreement to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Citation: Blockchain in Healthcare Today 2022, **5**: 196 - http://dx.doi.org/10.30953/bhty.v5.196

Acknowledgments

The authors acknowledge Professor Sarfraz Khurshid of the University of Texas at Austin and Bo Vargas for their guidance and support. For their assistance in assessing MediLinker's feasibility, the authors acknowledge Cole Holan, Cody Cowley, Jeremiah Alexander, and Alejandro Juul. They also thank all participants who interacted with MediLinker system in a simulated environment and helped in improving its design.

References

1. Congress of the United States. H.R. 34–114th Congress: 21st Century Cures Act. 2016. Congress.org. Available at: https://www.congress.gov/bill/114th-congress/house-bill/34
2. Dankar FK, Gergely M, Dankar SK. Informed consent in biomedical research. Comput Struct Biotechnol J. 2019;17:463–74. doi: 10.1016/j.csbj.2019.03.010
3. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Bitcoin; 2008. Available from: https://bitcoin.org/bitcoin.pdf, [cited 1 December 2021].
4. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. Proceedings 2016 2nd International Conference on Open and Big Data—Obd 2016. 2016:25–30.
5. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J. 2018;16:224–30. doi: 10.1016/j.csbj.2018.06.003
6. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc. 2017;24(6):1211–20. doi: 10.1093/jamia/ocx068
7. Mettler M. Blockchain technology in healthcare the revolution starts here. 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom). 2016: 520–2. Munich, Germany; 14–17 September 2016.
8. O'Donoghue O, Vazirani AA, Brindley D, Meinert E. Design choices and trade-offs in health care blockchain implementations: systematic review. J Med Internet Res. 2019;21(5):e12426. doi: 10.2196/12426
9. Roehrs A, da Costa CA, da Rosa Righi R. OmniPHR: a distributed architecture model to integrate personal health records. J Biomed Inform. 2017;71:70–81. doi: 10.1016/j.jbi.2017.05.012
10. Liang X, Zhao J, Shetty S, Liu J, Li D, editors. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); 8–13 October 2017.
11. Zhuang Y, Sheets L, Shae Z, Tsai JJP, Shyu CR. Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. AMIA Annu Symp Proc 2018. 2018:1167–75.
12. Wong DR, Bhattacharya S, Butte AJ. Prototype of running clinical trials in an untrustworthy environment using blockchain. Nat Commun. 2019;10(1):917. doi: 10.1038/s41467-019-08874-y
13. Raghavendra M. Can Blockchain technologies help tackle the opioid epidemic: a narrative review. Pain Med. 2019;20(10):1884–9. doi: 10.1093/pm/pny315
14. Hughes F, Morrow MJ. Blockchain and health care. Policy Polit Nurs Pract. 2019;20(1):4–7. doi: 10.1177/1527154419833570
15. Khurshid A, Holan C, Cowley C, et al. Designing and testing a blockchain application for patient identity management in healthcare. JAMIA Open. 2021;4(3). doi: 10.1093/jamiaopen/ooaa073
16. Texas Health and Human Services Commission. MPOA, Medical Power of Attorney. 2018. Available from: https://www.hhs.texas.gov/laws-regulations/forms/advance-directives/mpoa-medical-power-attorney, [cited 1 December 2021].
17. Khovratovich D, Law J. Sovrin: digital identities in the blockchain era. Github Commit by jasonalaw October. 2017, p. 17. Available at: https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/topics-and-advance-readings/Sovrin--digital-identities-in-the-blockchain-era.pdf
18. Khovratovich D, Law J. Sovrin: digital identities in the blockchain era. Github Commit by jasonalaw October. 2017, p. 17.
19. Sovrin Foundation. Available from: https://sovrin.org/
20. Tobin A, Reed D. The inevitable rise of self-sovereign identity. The Sovrin Foundation; 2016;29(2016). Available from: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
21. Hyperledger Indy. Type: Distributed ledger software. Copyright © 2022 The Linux Foundation®. Available from: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
22. Hyperledger Indy. Type: Distributed ledger software. Hyperledger Foundation. Copyright ©2022 The Linux Foundation®. Cited, 12/1/21. Available from: https://www.hyperledger.org/use/hyperledger-indy
23. World Wide Web Consortium (W3C). Copyright © 2022 W3C®. Available from: https:// www.w3.org/
24. React. A JavaScript library for building user interface. Copyright ©2022 Meta Platforms, Inc. Cited: 12/1/21. Available from: https://reactjs.org/
25. Naim NI. ReactJS: an open source JavaScript library for front-end development. Bachelor of Engineering, Helsinki Metropolia University of Applied Sciences; 2017.
26. React Native: Learn once, write anywhere. Cited: 12/1/21. Available from: https://reactnative.dev/
27. The React UI library you always wanted. React Native. Copyright ©2022 Meta Platforms, Inc. Cited: 12/1/21. Available from: https://reactnative.dev/
28. Merkel D. Docker: lightweight linux containers for consistent development and deployment. *Linux J*. 2014;2014(239):2.
29. Rhoades H, Wenzel SL, Rice E, Winetrobe H, Henwood B. No digital divide? Technology use among homeless adults. J Soc Distress Homeless. 2017;26(1):73–7. doi: 10.1080/10530789.2017.1305140
30. Raven MC, Kaplan LM, Rosenberg M, Tieu L, Guzman D, Kushel M. Mobile phone, computer, and internet use among older homeless adults: results from the HOPE HOME cohort study. JMIR Mhealth Uhealth. 2018;6(12):e10049. doi: 10.2196/10049
31. Menachemi N, Rahurkar S, Harle CA, Vest JR. The benefits of health information exchange: an updated systematic review. J Am Med Inform Assoc. 2018;25(9):1259–65. doi: 10.1093/jamia/ocy035
32. Wu H, LaRue EM. Linking the health data system in the U.S.: challenges to the benefits. Int J Nurs Sci. 2017;4(4):410–17. doi: 10.1016/j.ijnss.2017.09.006
33. Omar AA, Bhuiyan MZA, Basu A, Kiyomoto S, Rahman MS. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Generation Comput Syst. 2019;95:511–21. doi: 10.1016/j.future.2018.12.044

34. Dunphy P, Petitcolas FAP. A first look at identity management schemes on the blockchain. IEEE Security Privacy Magazine. 2018;16(4). doi: 10.1109/MSP.2018.3111247
35. 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. doi: 10.2196/10654
36. Khurshid A, Rajeswaren V, Andrews S. Using blockchain technology to mitigate challenges in service access for the homeless and data exchange between providers: qualitative study. J Med Internet Res. 2020;22(6):e16887. doi: 10.2196/16887
37. Khurshid A. Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. JMIR Med Inform. 2020;8(9):e20477. doi: 10.2196/20477