Future of Business and Finance

Chang Lu
Mohan Tanniru *Editors*

Blockchain in Healthcare

Analysis, Design and Implementation

Springer

Future of Business and Finance

The Future of Business and Finance book series features professional works aimed at defining, analyzing, and charting the future trends in these fields. The focus is mainly on strategic directions, technological advances, challenges and solutions which may affect the way we do business tomorrow, including the future of sustainability and governance practices. Mainly written by practitioners, consultants and academic thinkers, the books are intended to spark and inform further discussions and developments.

Chang Lu • Mohan Tanniru
Editors

Blockchain in Healthcare

Analysis, Design and Implementation

Springer

Editors
Chang Lu
Blockchain@UBC Research Cluster
University of British Columbia
Vancouver, BC, Canada

Mohan Tanniru
Department of Public Health Policy, Practice and Translational Research
College of Public Health,
University of Arizona
Phoenix, AZ, USA

ISSN 2662-2467 ISSN 2662-2475 (electronic)
Future of Business and Finance
ISBN 978-3-031-45338-0 ISBN 978-3-031-45339-7 (eBook)
https://doi.org/10.1007/978-3-031-45339-7

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgements

We acknowledge that this volume is a collective effort of all the chapter contributors and volume editors.

Contents

Role of Community Model in Networked Healthcare Organizations

Mohan Tanniru and Chang Lu

Abstract

Health care organizations have begun to engage in the digital transformation of their population health strategies to become patient centric by extending their care coordination into the client ecosystem using advanced technologies. Such transformation requires the engagement of an inter-organizational network of clinical and non-clinical partners and patients, as part of a community model. This community model needs a relationship governance capability to engage the partners to address shared health outcome goals, as well as a resource orchestration capability to share resources needed to create, fulfill, and assess care plans to achieve these outcomes. This chapter uses network and communication theories to discuss the formation of a community model in a networked organization, and blockchain technology can become a part of a digital platform used to address the evolving needs of patients. The last section discusses how various chapters in this book highlight the proposed use of blockchain technology for multiple healthcare networks as they address issues that are of interest to its community model actors.

M. Tanniru
Public Health Practice, Policy, and Translational Research Department, University of Arizona, Phoenix, AZ, USA
e-mail: mtanniru@arizona.edu

C. Lu (✉)
Blockchain@UBC, University of British Columbia, Vancouver, BC, Canada
e-mail: chang.lu@ubc.ca

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_1

1 Introduction

Organizations have begun to transform their operations with the use of digital age technologies by tailoring their services to meet evolving customer needs (Desmet et al., 2015). Service-dominant logic research argues that organizations must use transformations to engage with customers by creating services to support the customer purchase journey. This includes co-creating value with customers by developing innovative value propositions (products or services), fulfilling these value propositions with digital services quickly as a part of their digital strategy by leveraging technologies and external partner resources, and assess value in use by gathering feedback on evolving customer expectations and beginning the next value cycle (Vargo & Lusch, 2008; Lusch & Nambisan, 2015). To implement digital strategies with agility, organizations need a leadership that aligns business strategies around services for differentiation, a governance mechanism that manages partnerships and risks (Bharadwaj et al., 2013; Gray et al., 2013), and a digital platform to design and deliver services to meet customer expectations. Often called digital leadership or collaborative leadership across organizations (de Araujo, et al. 2021), it is viewed as an organizational capability (Peppard & Ward, 2004). It requires the engagement of different members of a leadership team to transform organizations based on the context and scope of the organizational change needed to create and sustain value to customers (Tanniru et al., 2018).

In the health care context, hospitals have started to extend their internal enterprise systems, such as electronic medical records, to a network of clinical care providers—including physician clinics, pharmacies, and skilled nursing homes—to reduce costs and improve care coordination post-discharge. Even if these providers create value (treatment or preventive practices), such-extended care coordination outside a provider ecosystem relies also on the engagement of patients and multiple social and community organizations that are not clinical but are critical to fulfilling the value so that the care can reach many patients with health disparities. Providers also rely on these non-clinical actors to assess value in use by gathering feedback to improve patient health outcomes. The growing use of technologies such as web-based portals, wearables, and other remote monitoring and teleconsultation technologies, is connecting diverse actors in the healthcare network. Health systems, external care providers (including social and community organizations), and patients face two major challenges in coordinating their activities to fulfill the value created (treatment adherence) and assessing value in use (gaps in adherence):

1. How to motivate and engage the diverse actors in the healthcare network to share the resources needed to support care coordination outside a provider ecosystem?
2. What digital platform or technology architecture is needed to connect diverse actors and technologies to share resources to support care coordination?

The challenge is to develop a system that supports coordination of care in a healthcare network through a system development lens. Such a system includes an analysis phase, where the requirements of the network actors to coordinate the care

are identified (*analysis of network actor requirements*), and a design phase, where a digital platform is developed to support the inter-organizational actors to share information to support care coordination (*inter-organizational technology architecture or digital platform design*), prior to implementation. We will discuss the analysis and design phases in Sects. 3 and 4. However, prior to discussing the analysis and design phases, we will illustrate in Sect. 2 four different strategies used by health systems to coordinate care to highlight the two challenges discussed above. These strategies are used in Sects. 3 and 4 as we highlight the analysis of requirements and design of digital platforms. Section 5 concludes this chapter and discusses how each chapter of this book maps to the analysis, design, and implementation of inter-organizational systems, using blockchain technology as a digital platform or considering it as a part of the digital platform.

2 Example of a Healthcare Network

Consider different health systems or hospitals that use point-to-point solutions, referred to as community strategies (CS), to address the health conditions of patients as part of care coordination using a mix of community actors (clinical and non-clinical partners, community organizations, and patients).

CS1 A health system used a remote care management system that connected high-risk patients living at home with hospital staff to communicate and share some vital sign information and used a local emergency management technician (EMT) to visit the patient at home for examination if health complications were observed.

CS2 A health system sent patients after cardiac surgery to a skilled nursing facility (SNF) for recuperative care before patients were discharged to their home. To improve the quality of care these patients received and reduce their potential readmission to the hospital, it partnered with a specialist team (a cardiac surgeon and an advanced nurse practitioner) to consult with the SNF staff when the patient condition became unstable and resolve any issues. If these issues cannot be resolved, the patients are then readmitted to the hospital.

CS3 A health system recognized that some of its patients were immigrants and/or poor and have diabetic conditions that need preventive care. It therefore provided them with glucose monitors and a mobile app on their phone so they could record their readings and share them with a community organization with which the health system partnered. The community organization showed healthy cooking using videos, tracked patient glucose levels, and answered any of their questions. It provided periodic reports on patient progress to the health system.

CS4 A health system recognized that some of its patients were obese and had high blood pressure. It referred the patients to a non-profit organization (called PHC here) that educated these patients on nutrition, physical activity, and behavioral health. It also provided them with digital tools, such as Fitbit, a

blood pressure cuff, and a weight scale, so they could record and report their progress to the educators. By addressing their barriers and improving their adherence to healthy behaviors, the PHC and its own partners supported their shared goal with the health system.

In summary, each health systems motivated its community actors to support the care coordination of patients by aligning each of their goals toward a shared outcome. In CS1, patients wanted care delivered to their home, and EMTs were willing to spend some of their waiting time to check on patients in their region for additional revenue. In CS2, both the SNF and the health system were motivated to reduce readmission costs by caring for cardiac patients at the SNF facility, and SNF staff needed additional skills provided by the specialist team for additional funding. Similarly, in CS3 and CS4, patients wanted to self-manage their health using digital tools, and health systems wanted to reduce their readmission costs. The community organization and PHC provided the preventive services as part of care coordination, as it is aligned with their organizational mission and additional support from the health systems.

To support resource sharing, each health system used different types of digital platforms with varying technologies to connect actors so they could share resources to coordinate care. For example, in CS1, the health system developed the digital platform that connected high-risk patients to remote monitoring tools and teleconsultation technology to patients and EMTs. In CS2 and CS4, the health systems distributed the responsibility of digital platform design to the SNF and PHC, respectively, so they could interact with their community partners and patients. In CS3, the health system developed the digital platform that allowed patients to interact with community organizations but distributed the data sharing responsibility using this digital platform to community actors: patients to track and share their glucose levels with community organizations, and community organizations to share educational videos and answer patients' questions.

Hence, as a part of addressing the challenges, the first step is to align the goals of each network actor so they can be motivated to support care coordination that will help a patient reach a desired health outcome, and to develop a digital platform that will connect actors so they can share their data/resources based on the context and capabilities of the actors involved. While such an approach to community strategy formulation to support the health needs of patients or population groups, as shown in Fig. 1, does address the needs at a given point in time, they are still point-to-point solutions with no agility to alter their network actors quickly when patient conditions change or when new technologies create opportunities for new services.

The need for such agility became apparent during the Covid-19 pandemic. During the pandemic, the demand for patient care has varied, sometimes calling for broadening clinical care or shifting from clinical to non-clinical care, such as addressing food, transportation, and economic insecurities. These changes required the inclusion of new social and community partners. In addition, when new technologies, such as telehealth, mobile apps, and wearables, entered the marketplace and found widespread use among clinical providers and patients, new services were possible that directly connected healthcare actors with patients, often bypassing some of the

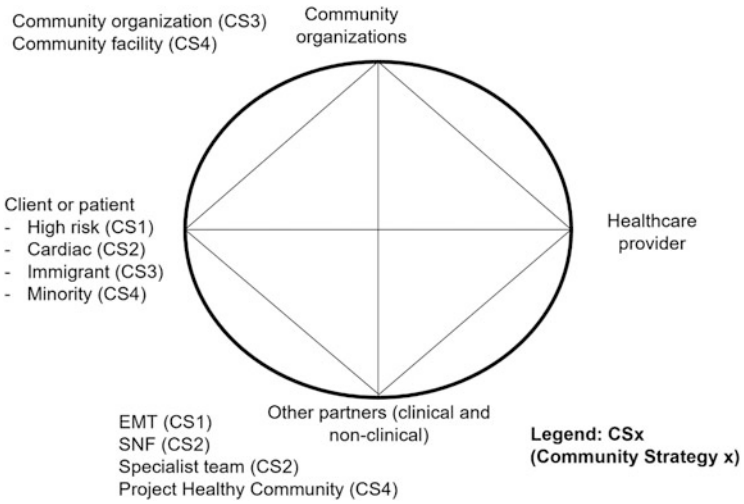


Fig. 1 Networks used to support different community strategies

community actors. Lastly, while the community strategies discussed here were developed by different health system, they can all be relevant for a single health system with multiple patients with similar conditions or when patients move from one health condition to another. For example, a patient released from an SNF (CS2) to home may be still treated as a high-risk patient calling for a change to a strategy with a new intermediary (CS1). Similarly, an immigrant or underserved patient who has diabetes and needs glucose monitoring (CS3) may also be diagnosed with obesity and hypertension, thus needing a new strategy with a different intermediary (CS4).

In summary, evolving changes in the patient ecosystem call for the development of an agile network model, called here a community model, to support care coordination. To address the dynamics of care coordination using such a community model, we rely on research on inter-organizational dynamics. Business organizations have used relationship management capabilities to leverage external partner resources to sustain competitive advantage (Moller & Svahn, 2009). They have started to look for inter-organizational dynamic capabilities (IDCs) to configure and re-configure the competencies of the firm and its partners to address changing market conditions (Teece, 2007). Sandberg et al. (2021) used prior research on IDCs to categorize four different IDC models along *two dimensions*: locus of control (who is the owner of the IDC) and beneficiary (who benefits from the use of the IDC), and *two IDC capabilities*: relationship governance and resource orchestration.

Based on these two dimensions, *exploitive and organization-based* IDC models have a focal firm controlling the coordination (or owner of the IDC model), and benefits accrue to the firm or firm and its partners. Both CS1 and CS3 can be viewed as organization-based IDC models, with health system controlling the care coordination. The other two IDC models, s*upportive and network based*, have the network

as the locus of control to coordinate member activities, and all network members benefit from the partnership. The network coordination can be done by either one or multiple members of the network based on the context, or else by someone from outside chosen by the network members. Both CS2 and CS4 can be viewed as supportive IDC models, with some members of the network sharing part of the care coordination (SNF or PHC). Network-based models or community-centric models in healthcare are either managed by an external party (a government agency or someone that the members agree to choose for such coordination) or else they can be an agile and find the right members to coordinate some or all the care coordination based on the context.

For our discussion in this chapter, we will consider the community model to be a network-based IDC model to support care coordination. In Sect. 3, we will use relationship governance capability to align the goals of all actors involved so they can see the benefit from participating in the network and be motivated to support care coordination. In Sect. 4, we will develop the digital platform with appropriate technology architecture based on actor competencies to support resource orchestration.

3 Analysis of Network Actor Requirements

Relationship governance is key to aligning the goals of all actors in a network and identifying their requirements, so that they are all motivated to participate and engage in working toward a shared goal of improving the health outcome of a patient population. If the actors in the network change as the health outcomes of patients evolve, then requirements must be extracted from current and new actors to sustain collaboration. Businesses extend their supply chain network to multiple partners when the market demands it, and achieving sustainable goals requires the participation and support of all supply chain partners. This becomes difficult when some of the partner nodes in the networks are far from the focal firm (Mamic, 2005) and inter-organizational capability to coordinate sustainability becomes a challenge (Egels-Zandén et al., 2015).

One of the inter-organizational dynamic capabilities is relationship governance, and a relational approach is suggested in managing supply chain networks (Andersson et al., 2022). Håkansson and Ford (2002) argue coordinating a long or complex network with diverse actors requires addressing three dualities: allow each member of the network to weigh the benefits of participating in the network against the constraints/costs of such participation; allow each to weigh their contribution of resources to influence the network against the influence the network will place on their own operations; and allow each member to evaluate the loss of their control over the resources shared with the network against the control they can exercise in helping the patient reach the planned health outcome. We will use these dualities to incentivize members to participate in care coordination as they engage in benefit–cost trade-offs, support transparent sharing of resources as they assess influence trade-offs, and help build trust that their resources are making an impact as they

assess control trade-offs. In other words, sustained collaboration among partners in community models calls for relationship governance that incentivizes participants and supports transparency while building trust to support care coordination.

Benefit–cost trade-off (incentivize) This requires supporting a members' decision to participate in the network and take advantage of the opportunities to share in the benefits (individually as well as patient outcomes) and overcome their constraints or the costs they incur (changing their operations to participate in the network). For example, in the SNF case (CS2), the hospital helped the SNF overcome its constraints (lack of staff skill) with the help of specialist team support, so it could realize the benefits of reduced patient readmission to the SNF. Similarly, the hospital helped the community organization overcome its technology constraint (CS3) by creating the tele-communication network, so it could track the glucose levels of patients and engage them in one-on-one consultation, while realizing the benefits of financial resources from the hospital as well as fulfilling its own mission.

Influence trade-off (support transparency) The second duality refers to the participating organization influencing the network even as it is influenced by the network (Gadde et al., 2003; Harrison & Prenkert, 2009). In care coordination, each node is asked to share resources with network partners by changing its operations and resource mix (influenced by the network), but the organization can also influence the efficacy of the care coordination strategy by ensuring that each node is contributing to the shared goal. In both the SNF (CS2) and PHP (CS4) cases, the health system distributed the responsibility of care coordination to clinical and non-clinical partners that influenced their operations and led them to contribute resources. Both the SNF and the PHP, however, knew that the health system tracked patient outcomes, and the specialist team and patient population contributed their resources to improve health conditions and/or health behavior. Unless there is a focal organization providing visionary leadership, transparency in what each member is contributing to the network and gaining from the network is key for success in sustained engagement and resource sharing, especially when the network actors come from diverse clinical and social backgrounds.

Control trade-off (build trust) The third duality refers to how organizations must balance their potential loss of control over the resources they contributed to the gain in understanding and potential control they can have as part of the care coordination path used to support the community strategy. This is especially critical when reaching a desired health outcome takes a long time, as in chronic care management or changing health behaviors. The use of short-term metrics to demonstrate progress can be effective in these cases (Gardner & Matviak, 2022). In each case discussed, short-term metrics did provide opportunities to build trust. Continual monitoring of patient progress in CS1, skill enhancement of SNF staff in CS2, improved A1C of patients participating in CS3, and improved tracking of weight and blood pressure of patients in CS4 provided short-term metrics to ensure that each partner controlled their part of the care coordination path or activities to build trust in the strategy used.

In summary, the relationship governance capability of a community model calls on each member to identify their interest in supporting the shared goal, their requirements to help them transform their operations to contribute resources, their need to know the share of resources contributed by others to support transparency, and the metrics that will build trust among all participants that their care coordination activities are continuing to reach the desired outcomes. The next section will look at the design of a digital platform to support resource orchestration through the communication of resources or information and the coordination of activities to support care.

4 Design of Digital Platform

Pitelis and Teece (2018) argue that contemporary multinational enterprises orchestrate the resources present in a network of firms, with the focal firm deciding on when and what resources should be deployed and changed if the network needs to change (Nenonen et al., 2018). While visionary leadership and sense-making are called on to leverage network resources to develop different business opportunities (Moller & Svahn, 2006; Nenonen et al., 2018), one still needs a shared vision and network partner engagement so that each partner can accrue benefits from network participation beyond what they would get when they operate on their own (Butler & Soontiens, 2015; Kay et al., 2018). Within a community model, a shared vision and partner engagement calls for collaboration and partnering to support the relationship governance as discussed in the previous section before we can begin to orchestrate how they share their resources to support transparency and build trust in the network they share. Before we discuss the network features to support resource orchestration, we will refer to some of the research on communication as a process to identify the actors who will contribute the resources.

Research on communicative constitution of organizations (CCO) does not view communication as something that happens within organizations or between organizational members across a network. Rather, it is a process around which organizations are constituted. That is, organization is an effect of communication not its predecessor (Blaschke, 2009), and elements of communication, rather than being fixed in advance, are reflexively constituted within the act of communication itself (Craig, 2000). In community models, the continually changing needs of patients determine what care coordination activities are required to support these patients first, and this then determines who the actors are and who can perform these activities. In other words, established forms of network analysis should be turned inside out, letting communication events or communicative processes look for actors or organizations who can support these events (Blaschke et al., 2012). Haug (2013) identifies two dimensions for these communicative processes: the activity dimension, which assesses performance of the communicative process, used here by identifying the resources needed to achieve the shared goals, and the structure dimension, which creates the space for such interactions to occur, i.e. the digital platform that supports the network.

Activity Dimension

Within the community model, the relationship model has identified the requirements of the actors who need to share resources required to support care coordination, once the activity dimensions identify who the actors are that can support the care coordination—the activity dimension. For example, the communicative processes required for high-risk patients who are residing at home (CS1) need remote monitoring of vital signs, frequent consultation to answer their questions, and an occasional visit by a professional who can physically check the patient for any anomalies that can be addressed at home. However, this can be also done by a homecare specialist who can remotely monitor a patient and send their staff to check for anomalies, or by a resident nurse or caregiver, living with the patient at an independent living facility, who is trained on clinical examination. Similarly, the care coordination of a cardiac patient post-discharge with some clinical oversight before they are discharged to home is done by SNF (CS2), or it can be done at home with a resident nurse supported by the same specialist team, if monitoring technologies are available. On the other hand, the preventive care of underserved populations is focused on reducing glucose levels using better nutrition, and a set of actors are used in CS3. If such preventive care expands to improving their physical activity and behavior health using health literacy education, then the actors may be expanded to include those in CS4.

No matter which community model with different network actors is deployed to support the evolving communication process needed to support care coordination activities, there is still the need to incentivize all the actors, once identified, to support the coordination and learn about their needs for transparency and trust-building, as discussed in the previous section. This brings us to the structure dimension.

Structure dimension

The structure dimension is used to identify the space needed to engage actors in the act of communication. Given that we are using inter-organizational actors, we need to align the technology used to support communication among actors with the technology used by the individual actors within their own ecosystem. This brings to surface the need for understanding how inter-organizational IT and data governance help address this alignment process.

Inter-organizational IT governance Within an organization, IT governance seeks to align the goals of single IT-related decisions to organizational use of IT. This means that the right people are making the right decisions, and these decisions are in alignment with organizational goals (Weill, 2004). This of course becomes a challenge in a network model when these individual organizational rights and responsibilities must be balanced against the inter-organizational goals of the actors in the network (Chan, 2002). At the inter-organizational level, the role of trust and complexity plays an important role (Spil et al., 2010; van den Broek & van Veenstra, 2015), and relational management is key to ensuring that the people and processes are identified to support resource orchestration among network members. Both

relational dependency (Sydow et al., 2009) and network research (Eschenbächer & Zarvic, 2012) have identified some evolutionary and contingency based approaches (Sambamurthy & Zmud, 1999) to address shared understanding on what is needed to support the communication needs of actors in support of care coordination, so that appropriate IT systems are used to support these communication needs. This means, allowing each member's IT system to connect to the digital platform so they can enter their information, knowing that such information is shared with others to support the desired outcome, as well ask to know that each is similarly sharing their information to build support transparency.

Inter-organizational data governance Similarly, given the diverse number of actors who sharing their information with others, data governance at the inter-organizational level calls for investigation of ecosystem data governance (van den Broek & van Veenstra, 2015; Markus & Bui, 2012; de Reuver & Bouwman, 2012), with ecosystems characterized by multiple autonomous organizations. The configuration of data governance is a fundamental control mechanism to influence the design, dynamics, and success of the collaboration (Dominick & Otto, 2021; de Prieelle et al., 2020), and right use and sharing of data are key aspects for generating value propositions (Oliveira & Lóscio, 2018; Attard et al., 2016) to address evolving context at the inter-organizational level (van den Broek & van Veenstra, 2015). Within a community model, with patient-centered outcomes focus and health quality improvement, research has called for gathering data governance requirements from diverse stakeholders (Kim et al., 2014), and identifying complementary or collective goals with interdependent capabilities between different organizations, so that multilateral data sharing can support collaborations (Lis & Otto, 2020; van den Broek & van Veenstra, 2015). Shared vision and values, as discussed under relational governance, are needed to strengthen the commitment of network ecosystem actors (Imperial, 2005) to help build trust to supporting the way data is produced, consumed, and shared by participating organizations in the network (Huber et al., 2017; Sarker et al., 2012).

In the four cases discussed in Sect. 2 (see Fig. 2), the community strategies that connect each actor with the network need IT governance to align the IT systems of the organization with the network architecture. Similarly, there is a need for data governance to ensure the right data is shared with all the right network partners to coordinate the care. The exact nature of the IT and data governance is left up to the network actors associated with the community model. For example, CS1 used a digital platform (the devices that monitor client condition and the network that connects clients and EMTs with hospital staff) is controlled and coordinated by the hospital, with transparency provided to both patients and EMTs on the information they are sharing is impacting the patient outcomes, and having the trust that the health system to ensure their data is secure and adheres to all privacy and security regulations. In the case of CS2 (SNF), the hospital and SNF used different platforms but connected these to share patient data. Then, SNF used its own digital platform to support both IT and data governance with its data and IT infrastructure used

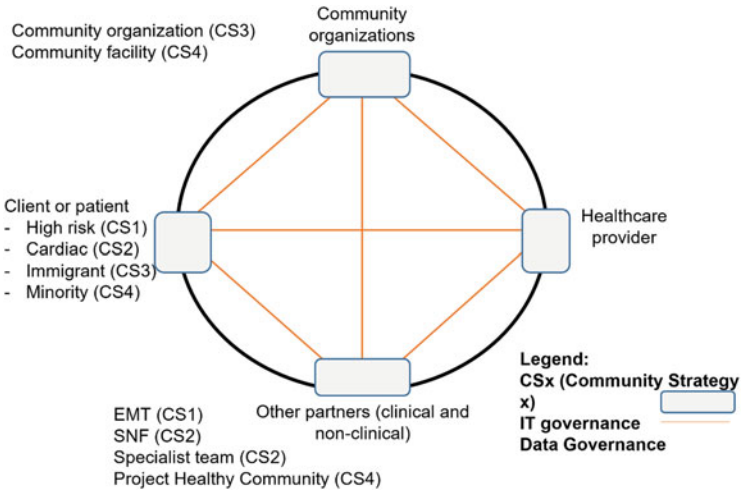


Fig. 2 IT and data governance to support community model digital platform

coordinate care of cardiac patients and interact with specialist teams. In both the CS3 and CS4 (PHC) cases, the community organization and PHC are responsible for data governance as they managed to use patient adherence data to support outcomes but have different IT governance mechanisms: health system governance the IT infrastructure in CS3, and PHC governed the IT infrastructure in CS4.

In summary, community informatics theory (Clement et al., 2012) posits that technology will not support community development if the community does not have the capacity to use the technology effectively, and effective use of technology is needed to accomplish collaborative goals (Gurstein et al., 2009). In each of the four cases, there has been an attempt to build capacity among the community actors, including clients or patients, to participate in the care coordination activities to improve health outcomes. Combining both the relationship building and resource orchestration capabilities, a community model can begin to identify the network actors (organizations, partners, and clients and their community) and help each actor make trade-offs on cost/benefits for contributing resources and knowledge (or data) using digital platforms but ensure the distributed IT and data governance capabilities of the network actors contribute to both transparency in the resource shared and trust that it is indeed contributing to improved patient outcomes. The exact nature of inter-organizational actor governance of IT and data may be shared among actors who have the capacity and the trust of those who are contributing to the community. Some of these networks may be coordinated by selected actors, or blockchain technology with peer-to-peer connectivity may be used when appropriate.

The rest of this chapter (the next section) will summarize some of the book's chapters and how they analyze the network actor requirements for sharing resources using blockchain technology as a platform. While chapter "Blockchain Architecture for the Healthcare Ecosystem" discusses the pros and cons of using blockchain

technology as a platform to support resource sharing, the rest of the chapters illustrate the use or proposed use of this technology by emphasizing various aspects of relational governance. Chapters "Blockchain-Based Dynamic Consent for Healthcare and Research", "Pay for Value": Blockchain for Drug Pricing in Canada", and "A Blockchain-Centric Data Sharing Framework for Building Trust in Healthcare Insurance" highlight the need for regulations and incentives to support actors in making value trade-offs in health data sharing, drug pricing, and health insurance. Chapters "Learning to Trust: Exploring the Relationship between Trust and User Experience in Blockchain Systems" and "Design and Implementation Considerations for Blockchain for Health Records" highlight the need for building transparency in the way resources are shared to support goal alignment through interface design and data privacy and security. Chapter "Blockchain Implementation for Decentralized Real-World Research" highlight the need for trust when resources are shared between pharmacies and patients, and the last chapter highlights the role of broader governance or even automated governance to align goals and share resources when network actors come from different constituencies with conflicting agendas, as in the case of health organizations and consortia representing various constituencies in health.

5 Summary of Chapters

The chapters begin with Garimella and Dutta's (chapter "Blockchain Architecture for the Healthcare Ecosystem") account of how blockchain may bring both tangible and intangible value to healthcare, and they present a framework for analyzing how such value may be materialized. They suggest that blockchain is not only suited, due to its technical advances, to addressing many of the tangible challenges in healthcare—including lack of automatic trust, need for privacy, and too much reconciliation—but also that the adoption of blockchain can prompt actors to rethink coordination networks and incentive alignment, resulting in unexpected positive change. They emphasize that both the business and technical architecture of blockchain must be considered to materialize the value of blockchain, where the business architecture is anchored in dimensions such as incentive design, governance framework, and rules of participation, since clarifying these dimensions is the first step toward motivating resource sharing and trust-building among actors in complex communities such as healthcare. Their chapter provides an overarching framework for the analysis, design, and implementation of blockchain adoption in healthcare.

In Charle's chapter (chapter "Blockchain-Based Dynamic Consent for Healthcare and Research"), the author draws attention to one of the most important resources for collaborations in digital health: health data. The author explains that in the current practice of health data management, individuals know little about how exactly their data is shared and used, and the chapter calls for a better protection of the "rights to data" through dynamic consent. Dynamic consent enables individuals to see the adaptations of research protocols and various data accessors in a transparent manner,

and it allows organizations to demonstrate consent evidence through immutable audit trails. The author suggests that blockchain-based dynamic consent can maximize the transparency and provenance of compliance of dynamic consent, especially by deploying smart contracts that allow individuals to make specifications as to who can access health information, when they can access it, and for what purpose. In addition, it saves organizational resources, such as manual labor, by automating dynamic consent and provides monetization to individuals whose data has been accessed by researchers. As such, blockchain-based dynamic consent is poised to not only improve trust toward health research, but also create better alignment between the incentives of individuals and researchers.

Kong et al.'s chapter (chapter ""Pay for Value": Blockchain for Drug Pricing in Canada") sensitizes us to the measurement and remittance of the value of the resources shared and transferred among actors in a pharmaceutical network, by examining blockchain for value-based drug pricing—a practice that aims to make drug prices fairer and reflective of its value to patients. Kong et al. examined the issue of transparency and consensus-making in drug pricing and demonstrated that the use of blockchain may help overcome the legal, economic, and policy barriers to value-based pricing. Focusing on drug pricing in Canada, the authors highlighted that the complex network of decision-makers and payers embedded in various levels of health administration renders the negotiation, settlement, and auditing of drug prices extremely difficult. On the one hand, this gives rise to the pressure of advancing value-based pricing, but on the other hand it makes the definition, measurement, and provenance of "value" almost unattainable. Nevertheless, connecting medical devices with pharmaceutical and medical records through blockchains and smart contracts promises a better capacity for different stakeholders to show the evidence of clinical improvements. It therefore lays the foundation for measuring and agreeing on the value of drugs and value-based pricing.

If Charle's and Kong et al.'s chapters mainly contribute to our understanding of analyzing the adoptability of distributed technologies (e.g., blockchain) for care coordination—by conducting the analysis in the context of dynamic consent and value-based pricing—Zhang et al. (chapter "A Blockchain-Centric Data Sharing Framework for Building Trust in Healthcare Insurance") shift the locus of contribution to how we may design distributed digital structures that are conducive to trust-building and resource sharing in healthcare. Using long-term care insurance as the context, they show that the design of such structures (blockchain-based specifically) would involve setting goals to reduce the risk of data tampering, system switching, and privacy leakage, and at the same time reduce the cost of transaction, transition, and verification. Such goal setting will be succeeded by matching different layers of the technology—API, smart contract, and zero-knowledge proof for identity and claim verification—to each goal. A perfectly matched architecture will result in increased trust among parties and more frequent and cost-effective sharing of a crucial resource: data.

While Zhang et al. focus on the back-end architecture design of blockchain-based information sharing for health insurance, Suleman and Lemieux (chapter "Learning to Trust: Exploring the Relationship between Trust and User Experience in

Blockchain Systems") draw our attention to the front-end user interface design of blockchain-based biomarker sharing by investigating the contributing factors in ensuring the trustworthiness of the interface. They suggest that since most individuals who use blockchain-based healthcare applications may not be concerned about the back-end engineering, their trust for the application may derive from their interaction with the user interface. Using both quantitative and qualitative methods, Suleman and Lemieux show that individuals may exhibit a stronger belief in the trustworthiness of the application when they are presented with features that convey a sense of information security, such as identity verification via QR codes, information about how their data will be used, and data sharing initiated by QR scanning. They also found that developing users' mental models that align with the application, in other words helping users understand the function of the application clearly, as well as engaging users in the design process through consultation and feedback, will help foster the belief of trustworthiness. In addition, when users are rewarded or their interaction with the application is rewarding, they tend to believe that the application is more trustworthy.

The next two chapters (chapters "Design and Implementation Considerations for Blockchain for Health Records" and "Blockchain Implementation for Decentralized Real-World Research") by Khambekar and Rhea et al. showcase pragmatic considerations for analyzing, designing, and implementing blockchain in healthcare, offering practice-informed recommendations that substantiate the theoretical insights in previous chapters. To begin, Khambekar suggest the following considerations for developing blockchain-based solutions: what stakeholders and what kinds of activities will be on or off the blockchain, what roles each stakeholder will play with respect to care coordination, which actor will have the right to read or write into the blockchain, who will pay the transaction fees, how health data will be stored on or off chain and how many blockchain copies will be created, which blockchain will be deployed, and so on. Then he provided useful recommendations, such as splitting health data into segments for more secure and duration off-chain storage, building solutions on open-source reputable blockchain protocols such as Hyperledger and Ethereum, crafting excellent user experience and engagement through education and quick response to users' needs, and building audit access to the blockchain. All these measures aim to ensure that stakeholders can trust the information sharing and storage on the blockchain, such that community-wide care coordination becomes seamless as information silos are overcome.

After Khambekar's chapter, Rhea et al. present a case study of implementing blockchain in healthcare, specifically focusing on the implementation of a blockchain-based real-world evidence (RWE) platform. The authors suggest that despite the unparalleled usefulness of RWE in pharmaceutical research, there has not been a sound infrastructure to incentivize patients to share RWE—defined as clinical and wellness data generated in everyday life, especially in a privacy-preserving and secure way. In their case study, Rhea et al. not only describe the technical architecture of the RWE platform, but, more importantly, share several implementation lessons. The most thought-provoking lesson is that patients may not need monetary incentives to share RWE, and incentives such as "share to earn" may prompt some

patients to game the system by sharing irrelevant data only to earn tokens. This insight alerts us to reconsider the incentivizing properties of blockchain-based applications, as the popular assumption is that blockchain brings about desired behaviors so long as some kind of tokens are allocated to the actors in question.

In the last chapter (chapter "The Inter-organizational Environment of Blockchain in Healthcare: The State of Blockchain Healthcare Consortia"), Trinh and Lu draw our attention to the organizational reality of blockchain adoption in healthcare by presenting a survey of existing blockchain-healthcare consortiums and uncovering their characteristics. As blockchain is by nature a peer-to-peer network, the implementation of blockchain solutions often requires collaborations between multiple organizations, and many efforts to adopt blockchain in healthcare are organized via consortiums. To some extent, consortiums are an inter-organizational apparatus by which actors deliberate the architecture of trust embedded in blockchains and configure small networks of resource exchange and incentivization. However, Trinh and Lu discovered that most of blockchain-healthcare consortiums are underdeveloped, as their objectives, governance models, and communications all seem to be ambiguous, a condition likely to result in organizational failure according to the literature on strategic alliances. The authors go on to suggest that consortium participants may consider algorithm-based governance in the form of decentralized autonomous organization (DAO), as such governance is native to blockchain. Since the field of healthcare is characterized by complex inter-organizational networks and inevitable information exchange among organizations, we believe that consortium is of critical importance to the adoption of most blockchain solutions, and scholars and practitioners must be aware of the current state of the consortiums and work toward a set of best practices.

6 Conclusions

Community model is well suited to help organize and coordinate care among healthcare organizations that are increasingly embedded in complex networks. However, in order for the effect of the community model to manifest, network actors must be aligned in their goals through proper incentives and governed in a transparent, participatory manner. While digital technologies such as blockchain hold the promise to improve incentive alignment and network governance, the technologies must be carefully designed and implemented. Insights into the design and implementation of blockchain for healthcare can be gained through the nine chapters in the present volume.

References

Andersson, S., Goran, S., Otero-Neira, C., Laurell, H., Lindgren, J., & Karlsson, N. (2022). Sustainable development considerations in supply chains: Firms' relationships with

stakeholders in their business sustainability practices—A triangular comparison. *Business Strategy and the Environment*. https://doi.org/10.1002/bse.3225

Attard, J., Orlandi, F., & Auer, S. (2016). *Data value networks: Enabling a new data ecosystem*. In IEEE/WIC/ACM International Conference on Web Intelligence.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Digital business strategy: toward a next generation of insights. *MIS Quarterly, 37*(2), 471–482.

Blaschke, S. (2009). *Building Blocks of Postmodern Organizational Communication*. Universitat Hamburg. Archived from the original March 2012.

Blaschke, S., Schoeneborn, D., & Seidl, D. (2012). Organizations as networks of communication episodes: Turning the network perspective inside out. *Organization Studies, 33*, 879–906.

Butler, B., & Soontiens, W. (2015). Offshoring of higher education services in strategic nets: A dynamic capabilities perspective. *Journal of World Business, 50*(3), 477–490. https://doi.org/10.1016/j.jwb.2014.08.001

Chan, Y. (2002). Why haven't we mastered alignment? The importance of the informal organization structure. *MIS Quarterly Executive, 1*(1), 97–112.

Clement, A. H., Gurstein, M., Longford, G., Moll, M., & Shade, L. (2012). *Connecting Canadians: Investigations in community informatics*. Athabasca University Press.

Craig, R. T. (2000, September 3). *Communication. Encyclopedia of Rhetoric*. Oxford University Press. Archived from the original on 20 December 2011. Retrieved 21 February 2012.

de Araujo, L. M., Priadana, S., Paramarta, V., & Sunarsi, D. (2021). Digital leadership in business organizations. *International Journal of Educational Administration, Management, and Leadership*, 45–56.

de Prieelle, F., de Reuver, M., & Rezaei, J. (2020). The role of ecosystem data governance in adoption of data platforms by Internet-of-Things data providers: Case of Dutch Horticulture Industry. *IEEE Trans. Eng. Manage* (pp. 1–11).

de Reuver, M., & Bouwman, H. (2012). Governance mechanisms for mobile service innovation in value networks. *Journal of Business Research, 65*(3), 347–354.

Desmet, D., Duncan, E., Scanlan, J., & Singer, M. (2015). Six building blocks for creating a high-performing digital enterprise. *McKinsey Digital*, September.

Dominick, L., & Otto, B. (2021). Towards a taxonomy of ecosystem data governance. In *Proceedings of the 54th Hawaii International Conference on System Sciences*

Egels-Zandén, N., Hulthén, K., & Wulff, G. (2015). Trade-offs in supply chain transparency: The case of Nudie Jeans Co. *Journal of Cleaner Production, 107*, 95–104.

Eschenbächer, J., & Zarvic, N. (2012). Towards the explanation of goal-oriented and opportunity-based networks of organizations. *Journal of Manufacturing Technology Management, 23*(8), 1071–1089.

Gadde, L.-E., Huemer, L., & Håkansson, H. (2003). Strategizing in industrial networks. *Industrial Marketing Management, 32*, 357–364. https://doi.org/10.1016/S0019-8501(03)00009-9

Gardner, H. K., & Matviak, I. (2022). Performance management shouldn't kill collaboration, employee performance management. *HBR, 9*.

Gray, P., El Sawy, O. A., Asper, G., & Thordarson, M. (2013). Realizing strategic value through center-edge digital transformation in consumer-centric industries. *MIS Quarterly Executive, 12*(1).

Gurstein, M., Beaton, B., & Sherlock, K. (2009). A community informatics model for e-services in Indigenous communities: The KNET approach to water treatment in northern Ontario. *Journal of Community Informatics, 5*(2).

Håkansson, H., & Ford, D. (2002). How should companies interact in business networks? *Journal of Business Research, 55*(2), 133–139.

Harrison, D., & Prenkert, F. (2009). Network strategizing trajectories within a planned strategy process. *Industrial Marketing Management, 38*(6), 662–670. https://doi.org/10.1016/j.indmarman.2009.05.012

Haug, C. (2013). Organizing spaces: Meeting arenas as a social movement infrastructure between organization, network, and institution. *Organization Studies, 34*, 705–732.

Huber, T. L., Kude, T., & Dibbern, J. (2017). Governance practices in platform ecosystems: Navigating tensions between cocreated value and governance costs. *Information Systems Research, 28*(3), 563–584.

Imperial, M. T. (2005). Using collaboration as a governance strategy. *Administration & Society, 37*(3), 281–320.

Kay, N., Leih, S., & Teece, D. (2018). The role of emergence in dynamic capabilities: A restatement of the framework and some possibilities for future research. *Long Range Planning, 27*(4), 623–638.

Kim, K. K., Browe, D. K., Logan, H. C., et al. (2014). Data governance requirements for distributed clinical research networks – Triangulating perspectives of diverse stakeholders. *Journal of the American Medical Informatics Association, 21*, 714–719.

Lis, D., & Otto, B. (2020). Data governance in data ecosystems – Insights from organizations. In *Proceedings of the 26th Americas Conference on Information Systems*.

Lusch, R. F., & Nambisan, S. (2015). Service innovation: A service-dominant logic perspective. *MIS Quarterly, 39*(1), 155–175.

Mamic, I. (2005). Managing global supply chain: The sports footwear, apparel and retail sectors. *Journal of Business Ethics, 59*, 81–100. https://doi.org/10.1007/s10551-005-3415-y

Markus, M. L., & Bui, Q. N. (2012). Going concerns: The governance of interorganizational coordination hubs. *Journal of Management Information Systems, 28*(4), 163–198.

Moller, K., & Svahn, S. (2006). Role of knowledge in value creation in business nets. *Journal of Management Studies, 43*(5), 985–1007. https://doi.org/10.1111/j.1467-6486.2006.00626.x

Moller, K., & Svahn, S. (2009). How to influence the birth of new business fields – Network perspective. *Industrial Marketing Management, 38*(4), 450.

Nenonen, S., Gummerus, J., & Sklyar, A. (2018). Gamechangers: Dynamic capabilities' influence on service ecosystems. *Journal of Service Management, 29*(4), 569–592. https://doi.org/10.1108/JOSM-02-2017-0025

Oliveira, M. I. S., & Lóscio, B. F. (2018). What is a data ecosystem? In dgo '18 (pp. 1–9).

Peppard, J., & Ward, J. (2004). Beyond strategic information systems: Towards an IS capability. *The Journal of Strategic Information Systems, 13*(2), 167–194.

Pitelis, C., & Teece, D. (2018). The new MNE: 'Orchestration' theory as envelope of 'Internationalization' theory. *Management International Review, 58*(4), 523–539. https://doi.org/10.1007/s11575-018-0346-2

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies, *23*(2), 261–290.

Sandberg, E., Kindström, D., & Haag, L. (2021). Delineating inter-organizational dynamic capabilities: A literature review and a conceptual framework. *Journal of Inter-Organizational Relationships*. https://doi.org/10.1080/26943980.2021.1939224

Sarker, S., Sarker, S., Sahaym, A., & Bjørn-Andersen, N. (2012). Exploring value cocreation in relationships between an ERP vendor and its partners: A revelatory case study. *MIS Quarterly, 36*(1), 317–338.

Spil, T., van den Broek, T., & Salmela, H. (2010). It takes two to Tango: The fit between network context and interorganizational strategic information systems planning. *International Journal of Strategic Information Technology and Applications, 1*(1), 23–41.

Sydow, J., Schreyögg, G., & Koch, J. (2009). Organizational path dependence: Opening the black box. *Academy of Management Review, 34*(4), 689–709.

Tanniru, M., Khuntia, J., & Weiner, J. (2018). Hospital leadership in support of digital transformation. *Pacific Asia Journal of Association of Information Systems, (PAJAIS), 10*(3).

Teece, D. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350. https://doi.org/10.1002/smj.640

van den Broek, T., & van Veenstra, A. F. (2015). Modes of governance in inter-organizational data collaborations. In *Proceedings of the 23rd European Conference on Information Systems*.
Vargo, S. L., & Lusch, R. F. (2008). Why "service"? *Journal of the Academy of Marketing Science, 36*(1), 25–38.
Weill, P. (2004). Don't just lead govern: How top-performing firms govern IT. *MIS Quarterly Executive, 3*(1), 1–17.

Dr. Mohan Tanniru is the Adjunct Professor in the Division of Public Health Practice and Translational Research in the Mel and Enid Zuckerman College of Public Health, University of Arizona, Tucson/Phoenix and a senior investigator in the Global Health Initiative at Henry Ford Health System in Detroit, MI. He is also an emeritus professor of MIS of Oakland University. He taught at the University of Arizona, Oakland University, Syracuse University, and the University of Wisconsin-Madison. He was the former Dean of the School of Business and the founding director of Applied Technology of Business Program at Oakland University, and the Department Head of MIS at the University of Arizona. His research covers areas like knowledge/decision support, IT strategy and systems and service modeling and more recently in digital health and healthcare leadership and management. He has published over 90 research articles and his work has appeared in journals such as ISR, MIS Quarterly, Decision Sciences, DSS, JMIS, IEEE Transactions on Engineering Management, Expert Systems and Applications, Information and Management, CACM, as well as Health Policy and Technology, Journal of Patient Satisfaction, Journal of Healthcare Management, and Journal of Healthcare Administration. He worked with several hospitals like Beaumont Health Systems, Ascension/Providence, Henry Ford Health System and St Joseph Mercy Health System/Trinity all in Michigan, and many major business organizations such as GM, Chrysler, Ford, Compuware, HP/EDS, Honeywell, Intel, SAP, and Raytheon among others.

Dr. Chang Lu is currently the cluster manager at Blockchain@UBC, the University of British Columbia, where he completed his postdoc research on blockchain adoption in healthcare. His theoretical research focuses on technology adoption, organization and institutional change, and the interplay between culture and power. He has published several articles on leading management journals and taught senior undergraduate and MBA students Organizational Strategy and Organizational Behavior. He serves as the supervisor of master and MBA students for their research projects, is currently creating education materials for executives about blockchain in healthcare. He earned his Ph.D. in Strategic Management and Organization, School of Business, from the University of Alberta. Prior to his academic career, he worked as an HR professional in China and Europe.

Blockchain Architecture for the Healthcare Ecosystem

Kiran Garimella and Kaushik Dutta

Abstract

The healthcare industry presents special challenges as an ecosystem due to the nature of incentives and goals of the various participants such as patients, payers, hospitals, doctors, insurers, pharmacies, pharma companies, governmental bodies, and regulators. Despite its importance to the quality of life, it is plagued by inefficient processes, duplications, and delays. While blockchain is not a panacea for all of healthcare's issues, it can go a long way in removing friction in data transactions, ensuring integrity of drugs and prescriptions, protecting patient data, making high-quality data available for research or case-based analysis, preventing fraud, and mitigating conflicting incentives. Blockchain's native capabilities of consensus-driven record of data, immutability of data, smart contracts for fluidity in processing, and ensuring authorization-driven access (with immutable audit trail) are tailor-made for moving healthcare into the next generation of sophistication. We recommend an approach to blockchain architecture driven by the business requirements of the healthcare ecosystem that leverages these native blockchain capabilities. We discuss the components of flexibility, trade-off, and safety.

1 Introduction

Healthcare is one of those topics, besides education, that polarizes people in their expectations, economics, and rights. The philosophical spectrum of attitudes ranges from free healthcare for all to patient-pays-all. In between are various forms of

K. Garimella (✉) · K. Dutta
School of Information Systems and Management, Muma College of Business, University of South Florida, Tampa, FL, USA
e-mail: kgarimella@usf.edu; duttak@usf.edu

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_2

subsidies and insurance with a confusing mix of allocations of payments and responsibilities. As if this were not enough, healthcare has one additional complication that the education sector does not: data privacy. While people flaunt their educational attainments, they want to keep their health data private.

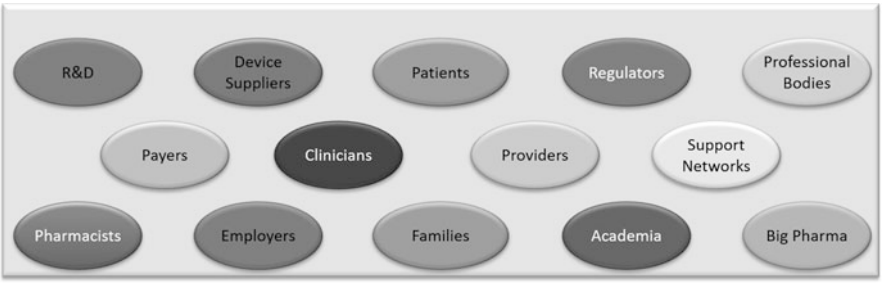
Information-sharing in the healthcare industry is characterized by the following attitudes and expectations:

- Patients don't want anyone besides their doctors to know about their health. Attitudes here differ in various cultures, ranging, as a broad generalization, from complete privacy in the West to relative openness in the East.
- Patients don't want their current doctor to know about their prior health issues if they see no bearing on the current health issue. A patient with diabetes who consults an ophthalmologist about an eye condition may not appreciate why he or she should disclose the condition of diabetes.
- Patients do not want their medical caregivers to know about the state of their finances.
- Doctors want to know everything about their patients' health to obtain a complete picture of their patients' health profile.
- Insurance companies want to know everything about the patients' health and finances to price their premiums and payments accurately.
- Patients would like to prevent their insurance company from knowing their pre-existing conditions (to the extent that their plans exclude coverage for pre-existing conditions).

The need to protect information and the need to know in the healthcare industry are driven, broadly speaking, by the following three considerations:

1. The practice of medicine (diagnosis and treatment)
2. Privacy
3. Economics of the healthcare

Healthcare has a huge number of participants with diverse goals, where the above three considerations form a complex, shifting tangle. These participants include the patients, their families (especially the main payer), primary care staff and medical professionals, specialists, doctors' practices, emergency care providers, insurance companies, pharmaceutical companies, wellness service providers, alternative medicine and holistic providers, supplement companies, hospitals, research organizations, consumer watchdogs, and government regulators.



According to a report by the Brookings Institution (Nunn et al., 2020), healthcare spending increased by 290% between 1980 and 2018, of which only 34% of the increase accounts for the aging population, leading to the situation where the healthcare industry that has relatively low productivity experiences rising costs. The report highlights the high proportion of administrative healthcare costs for nonclinical work such as "claims and payment processing, prior authorization and eligibility determinations, and quality measurement, among others." There are several reasons for these inefficiencies in healthcare which, from the perspective of blockchain technology, can be significantly reduced, if not entirely preventable.

An important reason for the poor cost management in healthcare is the lack of transparency for patients in total costs and quality of care prior to initiating the healthcare process. This introduces inefficiencies in the healthcare process as patients then have to dispute and debate the charges, at a time when they are most vulnerable, with the hospitals and insurers.

One other reason for healthcare inefficiencies and poor patient experience with the administrative processes of healthcare is the complex network of incentives that, from the patient's perspective, are misaligned. The patient wants the best care at the least cost, hospitals want to provide the best care in the most profitable way, the insurance companies want to increase their margins (which translates to lower coverage for the patient and less payment to the medical professionals). The confluence of these incentive structures results in many cases the limited amount of time doctors can spend (Rabin, 2014). The ability of blockchain technology to impact such incentives may be limited.

In Sect. 2, we review the foundational technologies of blockchain and describe their relevance to the problems faced in healthcare. The argument for the relevance of blockchain in healthcare is strengthened by an examination of the value it provides. In Sect. 3, we describe both the tangible and intangible value realized through adoption of blockchain. In Sect. 4, we show how the specific nature of problems in healthcare motivates the design of optimal architecture for blockchain applications, from a set of technology-agnostic business requirements to a set of implementation-agnostic technical architectural requirements. In Sect. 5, we describe various examples of blockchain applications in healthcare; these serve as exemplars or patterns of applications. In Sect. 6, we provide a brief description of the various types of applications of blockchain in healthcare. In Sect. 7, we describe the

main challenges in adopting blockchain in healthcare, such as data ownership, identity, privacy, and monitoring performance of contracts. In Sect. 8, we identify seven criteria that must be met to ensure successful adoption of blockchain in healthcare.

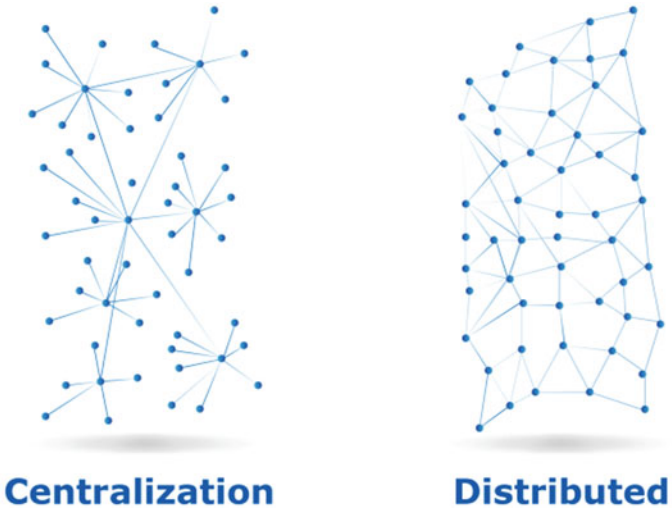
2 Blockchain for Healthcare Systems

Blockchain technology is not a panacea for all the problems of the healthcare industry. However, blockchain is tailor-made to address many of the issues that are peculiar to this industry. What are the specific characteristics of the healthcare industry that make them receptive to blockchain solutions?

The blockchain technology has two major components: distributed data and distributed processing. There is some confusion about the difference between decentralization and distributed systems. Blockchain per se is not about decentralization; rather, it is a distributed systems technology. The two terms, decentralized system and distributed system, are often confused, so much so that the term "blockchain" seems almost synonymous with a public, decentralized system.

2.1 Decentralized Versus Distributed Systems

The usual picture used to show the distinction between decentralized versus distributed systems is the one below:



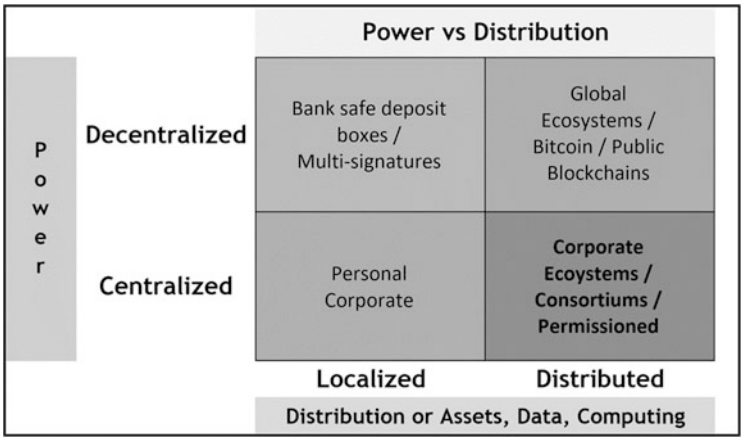
This picture is inadequate since it does not draw a clear distinction between decentralized and distributed systems. The terms "centralization" and

"decentralization" come with the baggage of value judgment and philosophy, while the phrase "distributed systems" has a purely technical connotation. Decentralization should be rightly used in the context of decision-making, power, authority, and control. Distributed systems are about geographical diversification of storage or processing. Centralization is about power, control, authority, accountability, and risk management. Distributed systems are about partitioning, dispersing, or part ownership of storage or computational capacity.

All decentralized systems are distributed practically by definition. However, not all distributed systems are decentralized. Enterprise systems at large companies can be distributed, but the company holds all the power and decision-making centrally. The other point to note is that centralization is not automatically evil, and decentralization is not automatically good. It depends on the context and the way an application is implemented.

Similarly, distributed systems are not automatically efficient. Poor architectural choices may provide none of the benefits of distributed systems and may increase vulnerabilities. Improperly designed incentives also have unintended consequences. For example, incentives for miners have concentrated power in the hands of large mining pool operators in Bitcoin and Ethereum networks, effectively pricing out individual participants. Centralization becomes a problem only if participants have an incentive to take unfair advantage and the system—by whatever name we call it—allows such manipulation. We also have to recognize that not all problems can be solved through technology alone. If that were true, there would be no need for partnerships, service-level agreements, intermediaries, and so on. The real challenge is to create an architecture that leverages technology in a cost-effective way while delegating the rest of the problems to the human institutions or social networks.

The figure below captures the nuances of centralized versus decentralized reframed as power versus distributed data and computing.



2.2 Relevance of Blockchain

The most effective way to design the right architecture for a blockchain to serve the healthcare ecosystem is to first understand the scope and applicability of blockchain for various types of problems. While there are several perspectives in determining applicability, we focus on two critical factors: scope and independence.

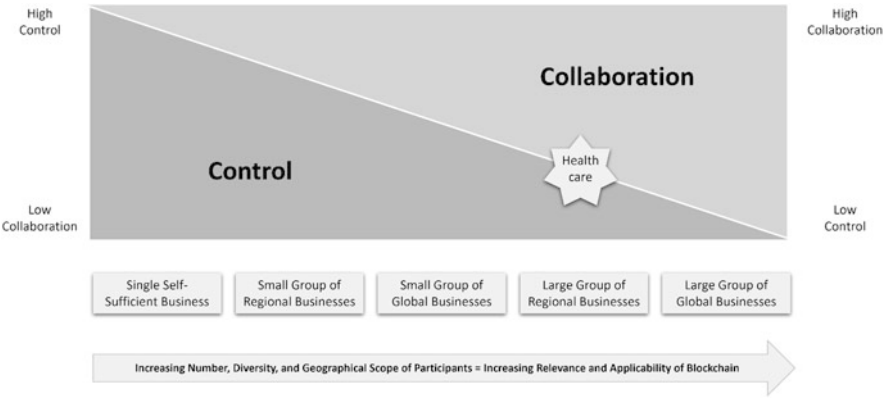
The scope of any technology, including blockchain, refers to the size of the underlying user base, which ranges from single users on one extreme to a global audience on the other extreme. The larger the user base, the more relevant is a blockchain solution.

Users in any industry prefer to have independence rather than be subject to rigid control by a central authority. Indeed, this is the premise of blockchain technology. Similar to scope, independence ranges from the single individual to groups of individuals who come together in a community with a shared vision or practice. When individual users form such a group, they voluntarily give up some independence to gain access to power and resources.

Since blockchain is most relevant in larger ecosystems where the participants have a common purpose, as in healthcare, a blockchain consortium is highly relevant and useful. A consortium provides a common governance process as well as applications, tools, and standards that benefit every member of the consortium. Examples of healthcare blockchain consortia include the Health Utility Network, Synaptic Health Alliance, and the U.S. Food and Drug Administration (FDA) (McFarlane, 2019).

2.3 Control and Collaboration in Blockchains

The trade-offs between control and collaboration tilt toward collaboration as the number, diversity, and geographical scope of the participants increase. The diagram below shows that blockchain is least relevant for single companies or a very small group of interrelated participants. As the number of participants increase, their geographical scope and dispersion increases as well since in modern supply chains it is rare for a large number of suppliers and customers to be concentrated in one small regional area. Moreover, modern supply chains are so interrelated that size automatically brings increased diversity of participants, each specializing in niche areas and providing value-added services.



3 Value of Blockchain in Healthcare

All the advantages of using blockchain in the healthcare industry are theoretically attractive. However, why should the individual participants adopt it? What specific values would it uncover to offset the cost of operating within a blockchain infrastructure? There are two major categories of value generated by blockchain, the tangible and the intangible values. Most practitioners in blockchain tend to focus exclusively on the tangible benefits. However, the intangible benefits are equally important, as will be described below.

3.1 The Tangible Value

The tangible value is in minimizing, if not eliminating, inefficiencies that cause leakage in value. This happens through inefficiencies in time, where participants have to hand-off transactions to the next entity in the business process chain.

A most significant example of this occurs in the manufacturing sector at GE Aircraft Engines. Maintenance of an aircraft engine requires unmounting it from the wing, carrying it to the maintenance shop, completing the maintenance, towing it back to the aircraft, and remounting it on to the wing. The unmounting, maintenance, and mounting were performed with world-class efficiencies. However, this still resulted in significant customer dissatisfaction because the total turnaround time was unacceptable and unpredictable. The inefficiencies were in the waiting to transport after unmounting the engine, waiting in the maintenance shop, waiting to transport the engine back to the aircraft, and waiting for technicians to arrive to mount it on to the wing (Kumar, 2013).

The immediate parallel to these inefficiencies is in the servicing of patients. Hospitals typically record the time the patient enters the treatment room until they are discharged, or even worse, only the actual duration of treatment or contact is

recorded. However, the patients' journey begins when they enter the hospital premises and ends when they exit the premises. In between are interminable periods of waiting.

Such inefficiencies are prevalent in the processing of transactions, as when medical records need to be shared between hospitals and bills are presented and allocated to various providers (the main inefficiency being with insurance claims). How can blockchain help in these situations? Blockchain's value lies in both distributed data and distributed processing.

Firstly, the data need not be transported since each node of the blockchain has immediate access to it. New data is synchronized between the various nodes in near real-time. Further, each entity is assured that the data has not been tampered with, thus fostering trust.

Secondly, the processing of transactions need not be "transported," since smart contracts "localize" the processing. At the same time, similar processing happens at the other nodes. Only when all the nodes compare the results of the processing and ensure they match perfectly (i.e., consensus is formed) will the results be cryptographically "sealed," distributed, and written immutably to the blockchain.

When this distributed data and processing is not available, the participants are reduced to waiting, unnecessary processing, and applying inconsistent rules or formulas. This requires constant reconciliation, restatements, and exchange of funds to cover discrepancies.

The first appeal to healthcare participants to adopt a common blockchain lies in exposing the myriad inefficiencies in processing and in reconciliation expenses (Gee & Spiro, 2019).

3.2 The Intangible Value

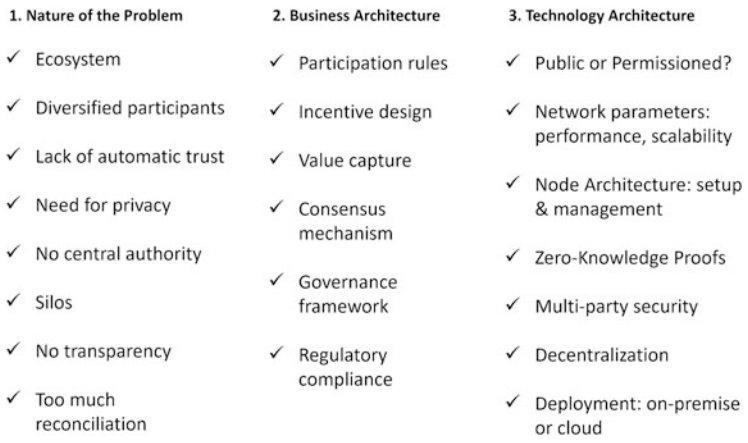
One of the most overlooked benefits of well-governed blockchain is its ability to foster dialog between the participants by making governance explicit and intentional. Setting up processes, designing revenue-share agreements, codifying them, debating updates to contracts, and other interactions related to the governance of blockchain facilitate collaborative dialog. This is generally true in all well-organized ecosystems. However, blockchain motivates a much more careful discussion since smart contracts, once deployed, generate immutable results. When there is no possibility of any of the participants changing the terms and conditions or putting their own interpretation on the clauses, they tend to be much more cautious while defining contracts and processes.

The call to adopt a blockchain solution for healthcare motivates the conversation on key segments of the industry where blockchain can address long-standing problems and facilitate the dialog to seek tangible value. The following section describes the process for creating blockchain solutions in the healthcare industry. We first review some of the key characteristics of the healthcare industry. Understanding them is the first step in determining the functional requirements of a blockchain solution (the "business architecture"). We then proceed to derive the technical

requirements for developing blockchain solutions without getting bogged down on the implementation details.

4 Designing the Optimal Blockchain Architecture for Healthcare

In this section, we describe how the nature of problems in healthcare influences an optimal design of the blockchain architecture. It is from the nature of the fundamental problem that the elements of the business architecture and technology architecture are derived. Without this grounding in the nature of the problem, there is a significant danger that the "shiny-object syndrome" of blockchain technology will lead the designers astray. We use the following generalized architectural design process for blockchain to motivate the development of a blockchain architecture for the healthcare ecosystem.



4.1 Nature of the Healthcare Problem

The healthcare industry faces a number of fundamental challenges. A good understanding of these problems will help in the design of a solution to address them effectively.

4.1.1 The Large and Diversified Healthcare Ecosystem

Healthcare is not a localized problem that is relevant only to a small group of participants or a small geographical area. There is a large ecosystem of many participants. The end consumer of the healthcare industry is the individual patient, who is generally mobile or changes employers numerous times. Blockchain too is

not a point solution. The larger the ecosystem the more relevant a blockchain-based solution becomes. Further, besides the sheer size of the ecosystem, the participants are loosely coupled and have no central authority except for some regulatory bodies that are themselves not organized efficiently. Compare this situation with a large, global conglomerate, which is also a large ecosystem, but which is much more constrained, controlled, and participants are fairly well-coupled, even if not technically integrated, with each other.

4.1.2 Diversified Participants

The participants in the healthcare ecosystem are widely diversified in terms of their size, influence, incentives, geographical scope, and influence.

4.1.3 Lack of Automatic Trust

The widespread, decoupled, and highly diversified set of participants that have no efficient and rallying regulatory constraints creates an atmosphere of distrust. Insurance companies want to limit costs and can dictate procedures. Doctors would like to select procedures that benefit the patient but may have constraints placed on them by the insurance companies. Medical practices and hospitals want to make money. Patients' incentives are complex and frequently contradictory given the trade-off between the best and most expensive procedures with the patients' desire to pay as little as possible.

4.1.4 Need for Privacy

The need for privacy conflicts with the need for transparency. This conflict results in wasted productivity in reconciliation of medical records, billing, collections, and miscellaneous data sharing.

4.1.5 No Central Authority

The lack of central authority makes it difficult to rally all the participants to a common vision, common standards, and consistent policies.

4.1.6 Silos

Both from various studies and from personal experience, data duplication, rekeying, and making paper copies are the defining experiential characteristics of the healthcare experience.

4.1.7 No Transparency

Patients have little insight into the cost versus quality tradeoff, or the fine nuances of effective treatments and risks. Silos create further barriers to information flow.

4.1.8 Too Much Reconciliation

The lack of consistent healthcare policies and siloed information leads to the inevitable nightmare of reconciliation.

These characteristics of the problem in healthcare are ripe for an immutable, auditable, multi-party distributed ledger with secure multi-party distributed processing. Evidently, this is the promise and the value of blockchain.

4.2 Deriving the Business Architecture for a Blockchain Solution

In this section, we describe what is meant by the business architecture of a blockchain solution in addressing the issues in healthcare. This is a prerequisite for implementing an effective solution.

The business architecture of a solution covers a technology-agnostic definition and description of the key functional elements that the solution is required to address. This approach ensures that the technology does not drive the solution, but that the right technology is selected based on the nature of the problem and the functional components required by the solution.

4.2.1 Participation Rules

Each of the healthcare participants need to work within the constraints of their business models, revenue-share arrangements, and regulatory constraints. These can be represented as "rules" and codified as smart contracts. Smart contracts run the same code on distributed nodes, owned by multiple parties, and ensure consensus. This addresses the major problem of continual reconciliation of records and goes a long way to resolve disputes (though not eliminate them entirely).

4.2.2 Incentives

Tied closely to codified contracts is the issue of incentive design. Improper incentives result in prescription of unnecessary medications and procedures, or in the avoidance of prescribing necessary procedures. Similarly, they result in fragmented procurement. Blockchain per se cannot prevent bad incentive design any more than technology can prevent a one-sided contract. However, blockchain can assist in making available immutable and auditable data that is generated by contracts. This enables investigators and researchers in evaluating the performance of contracts.

4.2.3 Value Capture

The adoption and sustained use of a blockchain solution requires that the smart contracts that represent incentives and business processes continually capture the value they generate. Value is defined as savings in time and cost, increase in quality (and corresponding reduction in adverse effects or relapses), improved patient experience, and increase in patient satisfaction.

4.2.4 Governance Framework

Blockchain forces stronger governance, since without the participants working together to extract mutual benefits a blockchain would not be possible. The infrastructure of blockchain in itself requires consensus during the process of creating

new contracts or updating existing arrangements. In other words, it is not possible for one entity to unilaterally release smart contracts that skew incentives in its favor.

4.2.5 Regulatory Compliance

A significant advantage of blockchain is in ensuring regulatory compliance. Regulators themselves could operate their own nodes and run verification algorithms. In fact, a strong governing body would ideally create smart contract templates that would be based on healthcare regulation. It is only blockchain technology that can ensure preventive measures such as these.

4.3 Technology Architecture of Blockchain for Healthcare

In this section, we describe the architectural components of blockchain for implementing a solution. The technical architecture is implementation-agnostic; it sets the parameters for a technical solution in a way that the solution meets the functional requirements of the solution (which, in turn, are derived from the nature of the problem).

4.3.1 Public or Permissioned

Since healthcare is regulated and carries significant potential for errors, misuse, and fraud, a permissioned blockchain is best suited for implementing a solution. Participants cannot be completely anonymous (as in a public chain). Medical professionals must be licensed, and patients should be able to check on their doctor's credentials.

4.3.2 Network Performance and Scalability

Permissioned blockchains can handle performance and scalability much better than public chains. Healthcare transactions are not random or speculative, as may happen in Bitcoin and Ethereum. Generally, performance is not an issue except for trauma care. Scalability and performance can be managed by spinning up additional nodes, creating "channels" (as is possible in the case of an industrial-strength permissioned blockchain such as Hyperledger Fabric). Unlike in public chains, nodes in this network are managed by regulated and licensed entities who have to conform to service-level agreements and reporting requirements.

4.3.3 Node Setup and Management

A permissioned blockchain automatically includes the infrastructure for credentialing and rights management. Patients themselves can be represented by a Patient Node and all patients can be credentialed under it. Other nodes can represent the various types of participants, such as doctors (with separate nodes for each specialty), nurses, hospital administrators, pharmacies, pharmacists, insurance companies, pharma companies, diagnostic centers, labs, logistics providers, regulators, lawyers, etc. The only additional work that is not native to blockchain

is the user interface and application. Each type of node requires a cloud-based web-application.

4.3.4 Zero-Knowledge Proofs

Privacy is an important consideration in the healthcare industry. In any interaction between two parties, one party must verify the claims of the other party. The party that is making a claim is conveying information about who they are, what they know, or what they can do. For example, a patient declares his or her age, prior diseases, medications obtained from another doctor, previous surgeries, etc. Medical staff need to know some information about the patient, but not all the details. Application of zero-knowledge proofs is an active area of research where the prover (the party making the claim) can prove to the verifier that he or she is, knows, or can do something without actually disclosing the underlying information (Sharma et al., 2020).

4.3.5 Multi-party Security

Sharing some information requires more than one party to provide approvals or to "unlock" it. Techniques that facilitate such multi-party sharing include homomorphic encryption and secure multi-party computation (Scheibner et al., 2021).

4.3.6 Decentralization

The concept of decentralization seems almost synonymous with blockchain. However, decentralization is an ideological goal in public blockchains. There is little incentive to achieve pure decentralization at the individual level within the healthcare industry. Instead, the various participants seek independent access to immutable information (within the constraints of privacy and need-to-know) and depend on the comfort of knowing that the records are fully auditable if necessary. The requirement within the healthcare industry is distributed data and partial decentralization just enough to prevent collusion to falsify records. Permissioned blockchain do not require full decentralization.

4.3.7 Deployment

Blockchain, by its nature, is best suited to deployment in the Cloud and taking advantage of the distributed nature of Cloud architecture. However, deployment of a blockchain node within premises does not contradict the blockchain architecture as it is agnostic to where the node is actually situated. Large companies may choose to host their node on their premises, but nodes are connected to other nodes in a way that protects independent consensus. Similarly, patient organizations and advocacy groups may host nodes on behalf of patients and provide application-level access to the patients.

5 Patterns in Blockchain Applications

There are several startups who have sought to address the problems in healthcare from various perspectives. Many have chosen to focus on specific areas while a few have elected to solve a "horizontal process" problem such as supply chain or on an infrastructure to power other point solutions. This is a rapidly evolving startup ecosystem. Examples cited at the time of writing may not survive as companies a few months or a year later. This is to be expected in a rich ecosystem that is rapidly innovating not only in the fundamental blockchain technology but also in the blockchain-driven innovation in disruptive healthcare business models.

It is illustrative to study visionary startups, not only for their successes but also for their failures. The blockchain architectural framework helps in analyzing the reasons for failure, such as improper definition of assets, lack of governance on transactions, improper incentives, over-ambitious smart contracts, or just a poor choice of technology.

Almost all of the blockchain solutions share similar characteristics and they overlap the problem areas. This is inevitable, since blockchain brings special capabilities, just as databases bring special focus to data management. There are two broad clusters of these solutions, one focusing on the sharing of healthcare data and the challenges of identity and ownership that entails, and the other focusing on the transactional, operational, and supply chain aspects of healthcare business processes. The latter includes traceability and regulation due to the nature of the healthcare industry.

5.1 Identity and Sharing of Health Data

The companies in the space focus on ways to share electronic data, safeguard identity, and protect privacy. They include the early startups such as MedicalChain (https://medicalchain.com/en/), Factom (now acquired and rebranded as Accumulate (https://accumulatenetwork.io/)), Patientory (https://patientory.com/), Guardtime (https://guardtime.com/), and BurstIQ (https://burstiq.com/).

Medicalchain focuses on a single point of truth for health records that are acquired and stored with high integrity. Doctors, laboratories, and hospitals can obtain patients' information while protecting their privacy. Patient data also has a record of the origin of data. Medicalchain also operates a telemedicine platform called MyClinic.com (https://about.myclinic.com/company/). Virtual consultations between doctors and patients are facilitated through the use of "Medtokens."

Accumulate (formerly Factom) began its journey as a data publishing and sharing layer on top of blockchains. Rather than just a solution, it is an identity-based blockchain protocol that enables identity management across multiple blockchains with human-readable addresses and hierarchies of keys for flexibility and security.

Accumulate is an example of a startup that set out to address a specific problem in healthcare—that of securely and privately sharing medical data on a need-to-know basis and pivoted to provide infrastructural solutions for identity management in

general. This type of pivoting is quite common in all startups; in healthcare, it shows how the general problems in other industries take on additional importance and sense of urgency as they adversely impact health and quality of life.

Patientory takes the approach of putting health data back in the hands of the patients and allow them to monitor the data and provide them actionable insights. It provides a complete historical data, ability to create a care plan, monitoring of health scores, etc. How does Patientory provide a single access to data that is typically in multiple provider portals? This is accomplished by the user accessing their data using the credentials of the provider portals and then associating the same with their own Patientory private key. These records are then stored securely on the PTOYMatrix blockchain network (https://ptoy.org/).

The idea is to not just give the users access to their data and the results of various tests and care management, but also integrate all this into the lifestyle of the user. For example, a care plan can include daily fitness activities, water drinking tracker, using the health score tracker statistics for motivation, and taking photos to store into the system and comparing them at various milestones in the care plan. This type of blockchain application is very customer-centric, where the customer is the user (or patient), not the rest of the healthcare establishment.

BurstIQ also promotes the idea that privacy and ownership rights should be respected, and trust becomes part of the solution by aligning incentives correctively. This is an explicit recognition that it is not enough to just provide a blockchain technology but also create a compelling business and economic framework of incentives. Their LifeGraph (https://burstiq.com/technology/) technology captures the digital DNA that include not only static data but also interactions with people, places, and things.

Blockchain's main value in distributing data and processing takes on an additional dimension of distributed intelligence in BurstIQ. As data and interactions are aggregated across a large ecosystem, machine learning algorithms can yield interesting insights. As the company puts it, their solution is AI-enabled and blockchain-secure.

Guardtime is another company that has taken the fundamental problem of sharing data securely and created specific solutions for healthcare. Working under a joint program of WHO (World Health Organization) and Estonia, Guardtime created VaccineGuard (https://guardtime.com/vaccineguard), a globally verifiable vaccination certification platform. This ensures the verification of vaccination and immunization records. However, being in the unique position of having access to such data across many health outbreaks in multiple countries, VaccineGuard enables data analytics to glean the progress and effectiveness of public health campaigns. In similar vein, this also helps vaccine manufacturers detect diversion of supplies and substitution with counterfeits, thus limiting liability in case of false claims. Finally, VaccineGuard also helps in tracking health parameters, recurrence, and prevalence after the inoculations.

This type of health-specific data sharing in a private and secure way helped the company create the HSX—Life Sciences solution to provide immutable audit trails of activities that touch patients' health care records. This initiative led to the creation

of the Real World Data Engine to share aggregate results of medicine use. This would normally be done through traditional data sharing arrangements, redacting personally identifiable information, and sharing data through a number of technical mechanisms. However, with the blockchain, this problem is simplified since the data need not be moved after the initial distribution and cryptographically locking it. In other words, HSX provides data visibility, not data movement.

Pokitdok (https://pokitdok.com/) provides a blockchain application called DokChain (https://pokitdok.com/dokchain/) which is a distributed network of transactions processors that deal with financial and healthcare data in this industry. The idea here is to quantify items of data and facilitate their exchange in a secure way. The privacy of information is secured by strong guarantees and the ability to audit all transactions. The DokChain leverages the fundamental characteristics of blockchain in an obvious way: cryptographic security to secure the data, distribute it to prevent single points of failure, automated ledger entries that eliminate paper processing, and allow patients to control access to their data through private keys.

5.2 Traceability, Supply Chain, and Regulation

The ownership, custody, and provenance of medical products have critical implications in detecting counterfeits, quality, avoiding liability, supporting sustainable labor practices, and ensuring regulatory compliance. Lack of traceability impacts not only the medical manufacturers but also patients who may be denied quality care or denied reimbursements in case of counterfeit medications.

One of the pioneers in addressing some of the problems that plague healthcare is Chronicled (https://www.chronicled.com/), a custodian of the Mediledger Network, whose focus is on providing a trust infrastructure for trading partners in the life sciences industry. Mediledger provides the framework for complex supply chains of drug movement from manufacture to the patient. Along the supply chain, there are the challenges of complicated pricing, complex contracts, and requirements for regulatory compliance. The variations are many and their management and reconciliation can be extremely difficult and significantly erode the value of the supply chain.

The Mediledger Network takes an infrastructural approach. It is a "Network as a Platform" on which specific solutions can be built, almost in the manner of composing new process flows based on the fundamental building blocks of the Network. Since blockchain by its very nature motivates an ecosystem type of thinking, the Network and its layer of point solutions spark the building of wider solutions that bring together a larger audience of healthcare participants, not only in terms of the number of such participants but also their diversity.

Chronicled itself provides examples of such solutions: contracts and chargebacks and product verification. The challenge of reconciliation is widely prevalent in all industries, but as discussed before, the challenge becomes much more serious and causes life or death repercussions in healthcare. Every hour and every dollar that is spent in reconciliation and chargeback errors is an hour and a dollar that is not available to serve the needs of patients. Chronicled recognized the power of smart

contracts to lock down allocations and chargebacks in an environment of trust, immutability, and consensus. The contracts and chargebacks solution cover roster management (Health Industry Numbers (https://www.hibcc.org/hin-system/), 340B for discounted drug pricing (https://www.aamc.org/news-insights/340b), and Drug Enforcement Numbers (Verisys, 2021)), communication of real-time updates to contractual provision, and enabling efficient claim adjudication through automatic management of credits and resubmissions for chargebacks. Closely related is the challenge of product verification. Chronicled's solution on the Mediledger enables real-time verification of prescription drugs against the manufacturer's specifications.

Neither of these solutions, or any others for that matter in any blockchain application, would get much traction without the active involvement of the participants in the governance of the blockchain network. The Mediledger Network facilitates strong governance through two working groups (revenue management and supply chain) and by the inclusion of well-established and respected companies in the healthcare space. These include AmerisourceBergen, Amgen, Bayer, Cardinal Health, Genentech, Gilead, McKesson, Pfizer, and others (https://www.mediledger.com/#https://www.chronicled.com/request-demo-copy).

Another such effort was initiated by Blockpharma (https://www.blockpharma.com/), based in France, which aims to solve the problem of drug traceability and counterfeiting, reducing the estimated 15% of fake drugs, through its solution built on CrystalChain (https://crystalchain.io/).

From a regulatory perspective, the CDC (https://www.cdc.gov/) (Centers for Disease Control and Prevention) is working on several projects to help the CDC track the onset of diseases, help detect the origins of diseases, and to track their spread. As Jim Nasr, chief software architect at the CDC's Center for Surveillance, Epidemiology, and Laboratory Services said, "While individual organizations in the public health network share the same overall mission, a complex mishmash of data usage agreements and government privacy rules dictate which members can access information and which ones can modify it. That slows things down. A number of additional, sometimes manual processes are needed to make sure the correct organization or person sent or received the right data, and that it was used correctly. A blockchain can automate these steps." (Orcutt, 2017)

6 Applications of Blockchain in Healthcare

In this section, we examine various blockchain applications in healthcare. They serve as exemplars of what is possible for addressing different types of issues.

6.1 Identity Management

For both patients and providers, establishing identify and controlling access to health records is an important capability (Javed et al., 2021). This problem is specific to identity itself (establishing who the participant is and what belongs to that

participant). The mechanisms for sharing that data with others is a different problem. Without a strong identity management infrastructure, the rest of the blockchain application becomes suspect.

6.2 Medical Data Sharing

The fundamental problem in the healthcare industry is that patient data exists in scattered silos with no infrastructure or incentives for systems integration for sharing. The multiple hops of data between systems leave open the possibility of errors, which is the third leading cause of death (Minemyer, 2016).

6.3 Medical Records Management

Besides sharing medical data, multiple parties constantly update medical records. Strictly speaking, prior data should never be overwritten. Further, all updates must be logged so that audits can be performed. Blockchain natively comes with immutability, thus preserving a historical view of transactions (or ledger entries). Interactions on the blockchain require private keys before they can be validated and committed to blocks. Cryptographic keys are tied to the identity of the participants. This ensures non-repudiable audit logs for all changes.

Related to the issue of managing the data, blockchain also comes with one additional tool that is powerful in preventing inconsistent updates. Similar to database constraints, which are localized to single applications, smart contracts can enforce the same contracts in a distributed environment. These smart contracts can embody rules that specify legitimate and consistent updates and invalidate inconsistent updates. This eliminates manual errors since the operators of the source systems are forced to fix the errors at the point of origination rather than dealing with them after the fact.

A blockchain platform allows the transfer of data securely between parties while maintaining ownership of the data at the point of origination. This data will be trusted since it is immutable and available to all authorized parties at any time. Blockchain can work in synergy with current EHR initiatives, making their infrastructure stronger.

6.4 Medicaid Management

Closely related and particularly relevant for the U.S. is the management of Medicaid programs. The Center for Medicare and Medicaid Services identified several of the more common errors and suggested some promising practices to prevent them (Common errors, 2015). These are described below in two broad categories since they exemplify the types of issues that blockchain can solve natively through smart contracts.

- *The number of units errors*: billed units differ from the number actually used in the procedure, billed units exceed the number authorized by the doctor, improper date spans are specified for administration, wrong procedure codes, wrong time segments recorded for administering the units, etc. In such errors, the key prevention mechanism within blockchain is the codification of the rules of calculations, administration, and duration for each of the procedure codes, encapsulated into smart contracts. Upon entry of the incorrect data, the smart contracts would prevent the propagation of these errors. Of course, similar validation can be performed by the providers' own applications, but the key premise of blockchain is that all the providers should design, test, certify, and agree to the common smart contract. So, regardless of how providers may wish to independently interpret these rules or how programmatic errors can be made, the final validation would identify these errors at source. The governance mechanism of blockchain would provide a forum for reviewing or updating with consensus the smart contracts or motivate continuous improvement in source systems.
- Improper documentation errors: key data required in filing of claims or allocation of costs among providers may be missing, changes in administration of units and progress notes are either missing, inadequate, or the authorizing signatures are missing. In such type of errors, smart contracts would encapsulate the minimum mandatory documents or pieces of data required to submit the case history. The issue of authorizing signatures is addressed by the requirement to use private keys to digitally sign the submitted information. Since blockchain keys are connected to the identity of the signer directly, the smart contracts can check to see if the signer is indeed authorized to sign the submission or not.

These types of errors in data and in the Medicaid processes can be significantly prevented by blockchain technology through the use of smart contracts that extend the normal validation functionality of localized databases into the distributed data ecosystem while also remaining agnostic to the database implementations.

6.5 Medical Supply Chain

The supply chain for healthcare can be compromised with adulterated, illicit drugs and drug trafficking (Committee on Understanding the Global Health Implications of Substandard, Falsified, and Counterfeit Medical Products, et al., 2013). Blockchain would help in maintaining a chain of custody and secure the provenance of the drugs and medical supplies. The traceability of drugs goes a long way in restoring trust in the healthcare industry (Uddin et al., 2021).

6.6 Medical Case Management

Since efficient tracking and sharing of information is a major problem in healthcare, there are significant opportunities for fraud. As much as 10% of healthcare costs are

deemed fraudulent. Compliance with billing codes is another problem that makes insurance coverage, billing, and payments full of reconciliation nightmares (National Heath Care Anti-Fraud Association, 2020).

6.7 Drug Development

In keeping with the common theme of lack of transparency and traceability of drugs and the process of development, the result is a strong counterfeit drug market that causes $200 billion annual losses (Howells, 2019).

6.8 Medical Research

Research and innovation in healthcare require sharing of clinical trial data. Half of all such research data is not shared or reported in any consistent way for availability (Watson, 2022). Blockchain obviously helps by providing a distributed data architecture that allows rapid sharing of trusted, immutable data.

7 Challenges in Implementing Blockchain in Healthcare

As in any large and worthwhile undertaking, adoption of blockchain in the healthcare industry has many roadblocks. Not all of them can be addressed by a technology solution such as a blockchain (or any other, for that matter). However, blockchain has several compelling "out of the box" value propositions that make it easier to overcome many of the objections.

7.1 Ownership of Data

As discussed in the earlier sections, the ownership of healthcare data is a thorny issue. This is not solely about patient data as commonly supposed. It also pertains to pricing arrangements, transactions, chargebacks, and insurance coverage. Each entity in the industry seeks to protect, withhold, and capitalize on data that originates with that entity.

The roadblock to adoption of blockchain is the misconception that putting data on the chain is tantamount to giving up ownership. However, blockchain is not a "socialist" or "communist" solution. Data ownership should be recognized and protected. If anything, blockchain can create immutable data ownership records by permanently and immutably associating the owner's cryptographic keys to the data. In essence, the data is permanently "stamped" with the owner's identity.

7.2 Identity

Ownership begs the question of identity—how to ensure that the owner of the data is a credible entity (individual or organization) and how that entity can be authenticated and their access to data and transactions authorized. Only a credible entity can be trusted to provide credible source data and engage in legitimate transactions. It must be noted that blockchain by itself cannot prevent all types of frauds and errors. Instead, blockchain's value lies in tying ownership, identity, and information immutably and inseparably.

The roadblock to adoption is the misconception that the public blockchains are the only type of blockchain available and that the participants in the public blockchains are anonymous and, more significantly, unverified or unverifiable. The latter is somewhat true (since there is no true anonymity in the public chains), but the former assumption is not. Most enterprise or business-related blockchains are permissioned or private, where unverified and anonymous entities cannot participate.

A robust and verifiable identity solution requires the following: establishing a KYC (Know Your Customer) ID verification which includes checking sanction lists, blacklists, and watchlists; re-verifying in case of material changes to the entity's KYC-related information, such as address, phone number, proof of government-issued identity documents (for example, driver's license or passport), corporate registrations, and so on, where the changes are either initiated by the entity or the underlying data has expired; and continual monitoring of sanction lists and bad actor lists. Many current solutions, whether based on blockchain or not, also include reputation scores from online activity including but not limited to social media and publications (Simons, 2021).

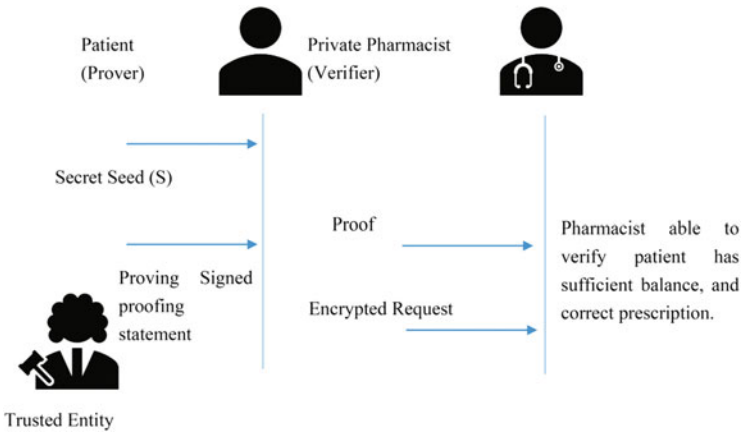
7.3 Privacy

Closely related to the issue of ownership is privacy. Who is entitled to know any particular information? Should an ophthalmologist know about the patient's gastrointestinal problems? Should a dispensing pharmacist have access to a patient's medical conditions that have nothing to do with the prescription at hand? Should the patient admissions personnel at a hospital be privy to a patient's embarrassing medical conditions? These questions are sensitive especially in cases of medical conditions that carry a social stigma, such as HIV, STDs, abortions, etc. The question of privacy also includes information not related directly to the patients. How much of the contractual arrangements between two parties be made visible to another party? In all these cases, the essential requirement of privacy is the need-to-know principle: Is it necessary for the service provider to know the information in order to provide effective service?

The roadblock to adoption is the misconception that all the data is out there on the blockchain for every participant to see. Fortunately, blockchain has several mechanisms, depending on the underlying technology, to enforce privacy and the

need-to-know principle. For example, Hyperledger Fabric, a permissioned, open source blockchain, has provision for creating sharing channels as well as private data collections. These mechanisms expose data only to those who need to know and the data within the channel is not available to any participant that does not belong to that channel. Blockchain can also incorporate general algorithms for zero-knowledge proofs (ZKPs (Wikipedia, 2022)), or in many cases more accurately, limited-knowledge proofs. ZKPs allow a party (the "prover") to demonstrate to another party (the "verifier") that it knows something or can do something without disclosing what it knows or how it can perform the action. Another mechanism for protecting privacy is the concept of multi-signatures, where multiple parties must authorize the disclosure of information. This can be effective when the parties include the original owner of the data, the caregiver, and an independent governing entity.

An example of a ZKP solution is the one proposed in "BZKP: Blockchain-based zero knowledge proof for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation" (Al-Aswad et al., 2021), in the figure below.



7.4 Performance of Contracts

While data is important, most organizations need to use that data in their transactions. These transactions in their turn generate derivative data. Participants in the supply chain originate other data at different points in time. All of this data is continually updated. Transactions need to follow certain business rules. When the business rules embody contractual relationships, the ability to manage contracts becomes a significant challenge.

The roadblock to adoption of blockchain are two opposing misconceptions: ignorance of and hype about the role of blockchain in contract management. The first misconception is that blockchain is all about data and being ignorant of its

potential for transforming the processing of that data (Iansiti & Lakhani, 2017). This is a lack of recognition of the concept of smart contracts and how the blockchain technology facilitates not only the distribution of data in the form of a distributed ledger but also the distribution of transaction processing.

The second misconception is to assume that blockchain's smart contract technology facilitates the rock-solid legal contracts that are fully imbued with sophisticated artificial intelligence. This is generally not true (Casper et al., 2021). This misconception arose in the early days of unreasonable expectations that smart contracts will replace lawyers entirely (the "contract" part) and fully automate the execution and performance monitoring of contracts (the "smart" part). At best, smart contracts up to this point in time are largely unsophisticated implementations of a few simple rules, most notably the avoidance of double-spend and checking for balances or comparing entities against a whitelist of permitted participants.

However, smart contracts do have a robust future that is possible only with a stronger implementation of contract law combined with true artificial intelligence and data analytic capabilities. In the interim, smart contracts can be used in a limited way to automate simple processing of contractual clauses, relegating the complex clauses to manual inspection.

8 Success Criteria for Blockchain Effectiveness in Healthcare

In order for blockchain to be effective in the healthcare industry, several criteria must be met. These criteria are directly related to the unique value proposition of blockchain in general and in its applicability to the healthcare industry.

8.1 Criterion 1: Collaboration

The blockchain solution or network must offer a collegial platform for a large number of participants. Blockchain is not an efficient solution for just a few participants.

8.2 Criterion 2: Diversity

It must offer a collegial platform for a diverse set of participants. If all participants are of one type, such as only pharma companies, only hospitals, only pharmacies, or only patient advocacy groups, the blockchain cannot facilitate supply chain solutions.

8.3 Criterion 3: Infrastructure

It must offer an infrastructural capability on which participants or value-adding organizations can collaborate to build solutions with the assurance that the underlying "motherboard" provides the safety guide rails of immutability, consensus, and trust.

8.4 Criterion 4: Smart Contracts

It must provide for authoring, implementing, and managing smart contracts. This is an often overlooked or underutilized power of blockchain. This is partly due to some misconceptions around the phrase "smart contracts," which in their current form are neither particularly smart (i.e., in the sense of artificial intelligence) nor actual legal contracts. However, in the context of rules of operation, metrics, and formulas, smart contracts serve to solidify contractual relationships with more clarity and automated performance than paper-based contracts.

8.5 Criterion 5: Incentives

It must enable the definition, implementation, and management of economic incentives among the participants. While this may seem to be solely the province of smart contracts, it also requires a forum for defining the incentives.

8.6 Criterion 6: Governance

It must provide for strong governance and active engagement of the participants. This can happen in many ways, from the traditional mechanism of working groups to the blockchain's specific advantage of requiring consensus for the definition of smart contracts and solutions.

8.7 Criterion 7: Innovation

It must provide an environment and a set of infrastructural tools for innovation and experimentation of new processes and business models. This is done through a growing collection of tools, standards, protocols, and one or more testnets for experimentation.

9 Future Directions

An effective blockchain architecture for the healthcare ecosystem depends on a diverse set of participants collaborating on data sharing and complete visibility into transactions. However, because participants are grouped together by region, healthcare vertical, and supply-chain segmentation, it is natural that each group evolves its own architecture. To become truly effective, a unifying force that facilitates the development and use of an interoperable architecture is required. To give a fictitious example, a blockchain for pharmacies need to connect to a blockchain for the New England Diabetics Association, and both need to connect to the California Heart blockchain. The advantage of such interconnectivity is that a heart patient who is a client of one pharmacy and living in New Hampshire moves to California and signs up with a more convenient pharmacy and needs to be treated for a heart condition will be served well when the interoperating blockchains cooperate to exchange relevant information without the time-consuming and tedious task of the new providers requesting health records from the previous providers and consolidating them in their systems.

Since healthcare is a well-regulated industry, the government agencies can become that unifying force. They can provide education, sponsor interoperability projects, and provide tax incentives for adopting interoperable blockchain solutions. Included in this interoperability should be strong mandates for maintaining privacy of patient data, implementing need-to-know sharing or zero-knowledge verifications and proofs, and strong security. Government agencies that focus primarily on research can help by providing grants in the above topics.

Significant areas of research include interoperability of blockchains using standards development and technology innovations such as blockchain oracles, multi-party signatures, zero-knowledge proofs, and parallel and independent audit chains.

10 Conclusion

The healthcare industry suffers from long-standing problems in data sharing and business processes that are the result of a complex mesh of incentives, contractual relationships, regulatory constraints, and convoluted financial accountability. These problems are difficult to address using traditional technologies which merely provide band-aid solutions that are either ephemeral or merely shift the inefficiencies downstream.

Blockchain technology offers a radically new approach through its distributed data and processing capabilities where all parties are coordinated through cryptographic consensus. More than just the technology, the process of implementing it motivates the participants to collaborate in the design of smart contracts and business processes.

While blockchain is not a panacea for all the ills of the healthcare industry, its special characteristics make it highly relevant and effective for addressing many

of the problems. In order to do this successfully, thought leaders who wish to explore blockchain for healthcare must be cognizant of the roadblocks and the essential criteria for its success.

References

Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). *BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation*. https://doi.org/10.1080/25765299.2020.1870812

Casper, R. H., Lazaro, J. A., Vogel, P., Wang, E., & Wegrzyn, K. E. (2021). Smart supply chains using smart contracts. *The National Law Review*. https://www.natlawreview.com/article/smart-supply-chains-using-smart-contracts

Committee on Understanding the Global Health Implications of Substandard, Falsified, and Counterfeit Medical Products, Buckley, G. J., & Gostin, L. O. (Eds.). (2013). *Countering the problem of falsified and substandard drugs*. Board on Global Health, Institute of Medicine. https://www.ncbi.nlm.nih.gov/books/NBK202523/

Common errors that lead to improper payments for home health services and agency-provided supplies, equipment, and appliances (2015). https://www.cms.gov/files/document/hcbs-common-errors-imppay-factsheet-102815pdf

Gee, E., & Spiro, T. (2019). *Excess administrative costs burden the U.S. healthcare system*. https://www.americanprogress.org/article/excess-administrative-costs-burden-u-s-health-care-system/

Howells, R. (2019). *Counterfeit drugs: A bitter pill to swallow*. https://www.forbes.com/sites/sap/2019/10/03/counterfeit-drugs-a-bitter-pill-to-swallow/?sh=76189b907a68

https://about.myclinic.com/company/

https://accumulatenetwork.io/

https://burstiq.com/

https://burstiq.com/technology/

https://crystalchain.io/

https://guardtime.com/

https://guardtime.com/vaccineguard

https://medicalchain.com/en/

https://patientory.com/

https://pokitdok.com/

https://pokitdok.com/dokchain/

https://ptoy.org/

https://www.aamc.org/news-insights/340b

https://www.blockpharma.com/

https://www.cdc.gov/

https://www.chronicled.com/

https://www.hibcc.org/hin-system/

https://www.mediledger.com/#https://www.chronicled.com/request-demo-copy

Iansiti, M., & Lakhani, K. R. (2017). *The truth about blockchain*. https://hbr.org/2017/01/the-truth-about-blockchain

Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., & Qureshi, K. N. (2021). *Health-ID: A blockchain-based decentralized identity management for remote healthcare*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8230390/

Kumar, R. (2013). *GE's early days with six sigma*. https://luminisindia.com/process-management-blog/129-ge-s-early-days-with-six-sigma

McFarlane, C. (2019). *Healthcare and blockchain: The impact of consortia*. https://www.forbes.com/sites/chrissamcfarlane/2019/03/14/health-care-and-blockchain-the-impact-of-consortia/?sh=7502030935b1

Minemyer, P. (2016). *Medical errors officially the third leading cause of death in U.S., study finds*. https://www.fiercehealthcare.com/healthcare/medical-errors-officially-third-leading-cause-death-u-s-study-finds#:~:text=Providers-,Medical%20errors%20officially%20the%20third%20leading,death%20in%20U.S.%2C%20study%20finds&text=A%20new%20study%20published%20in,only%20heart%20disease%20and%20cancer

National Heath Care Anti-Fraud Association. (2020). *The challenge of health care fraud*. https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/

Nunn, R., Parsons, J., & Shambaugh, J. (2020). *A dozen facts about the economics of the US health-care system*. https://www.brookings.edu/research/a-dozen-facts-about-the-economics-of-the-u-s-health-care-system/

Orcutt, M. (2017). *Why the CDC wants in on blockchain*. https://www.technologyreview.com/2017/10/02/148864/why-the-cdc-wants-in-on-blockchain/

Rabin, R. C. (2014). *15-minute visits take a toll on the doctor-patient relationship*. https://khn.org/news/15-minute-doctor-visits/

Scheibner, J., Raisaro, J. L., Troncoso-Pastoriza, J. R., Ianca, M., Fellay, J., Vayena, E., & Hubaux, J.-P. (2021). *Revolutionizing medical data sharing using advanced privacy-enhancing technologies: Technical, legal, and ethical synthesis*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7952236/

Sharma, B., Halder, R., & Singh, J. (2020). Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption. In *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Bengaluru (pp. 1–6). https://doi.org/10.1109/COMSNETS48256.2020.9027413

Simons, T. (2021). *Legal requirements for adverse media screening*. https://legal.thomsonreuters.com/en/insights/articles/legal-requirements-for-adverse-media-screening

Uddin, M., Salah, K., Jayaraman, R., Pesic, S., & Ellahham, S. (2021). Blockchain for drug traceability: Architectures and open challenges. *Health Informatics Journal, 27*(2): 14604582211011228. https://doi.org/10.1177/14604582211011228

Verisys. (2021). *What are DEA numbers and what are they used for*. https://verisys.com/what-are-dea-numbers-and-what-are-they-used-for/

Watson, C. (2022). *Many researchers say they'll share data – but don't*. https://www.nature.com/articles/d41586-022-01692-1

Wikipedia. (2022). *Zero-knowledge proof*. https://en.wikipedia.org/wiki/Zero-knowledge_proof

Kiran K. Garimella received a Ph.D. degree in Decision and Information Sciences from the Warrington College of Business, University of Florida. He is an Assistant Professor of Instruction at the Muma College of Business, University of South Florida. He has held roles such as Global CIO and Chief Architect at a General Electric company, VP and Chief Evangelist for Business Process Management at Software AG, and Chief Scientist and CTO at KoreConX. He is the author of three books, two chapters, several articles in conferences and reviewed proceedings, and has executive consulting experience in 20 countries. His research interests include safety and governance in enterprise blockchains, business and economic frameworks for data analytics, and the application of mathematical methods in analytics.

Kaushik Dutta received a Ph.D. degree in Management Information Systems from the Georgia Institute of Technology. He is a professor (Muma Fellow) and Associate Dean at the Muma College of Business, University of South Florida. He held executive roles such as VP of Engineering at Walkingstick Solutions, Inc., CTO and VP of Engineering, the current chief technical advisor at Mobilewalla, Inc., and a Business Mentor at the NSF I-Corps, University of South Florida Tampa

Site. He is the author of 40 peer-reviewed journal publications, 73 peer-reviewed conference publications, six journal papers in the UTD24 journal list, eight journal papers in the ABDC A* journal list, and premier journals, such as Information Science, Data Mining and Analysis, and Operations Research. His research interests include data-management applications in fintech, mobile advertising, and healthcare.

Blockchain-Based Dynamic Consent for Healthcare and Research

Wendy M. Charles

Abstract

As individuals gain greater access control over their health information, dynamic consent solutions are increasingly offered to allow individuals to make informed choices about their permissions over time. Blockchain-based tools and technologies are emerging to enhance the capabilities of dynamic consent solutions to offer individuals more engagement. While blockchain-based systems cannot replace all human interactions, blockchain features can increase granularity, transparency, and trust. This chapter describes the benefits and drawbacks of dynamic, informed consent and proposes several design and feature considerations to optimize blockchain-based features.

1 Introduction

An individual's informed consent (or permission) to collect, use, or share sensitive information is a cornerstone for the lawful processing of personally identifiable information. Furthermore, the ability to make an informed decision regarding the use of private information can be regarded as a person's "right" in Westernized cultures (Asghar & Russello, 2012). The tenet of this freedom demonstrates individual dignity, autonomy, privacy, and integrity by respecting someone as a person (Cheung, 2018).

Informed consent can be defined in several ways depending on the applicable laws and contexts in which informed consent is obtained. Definitions of informed

W. M. Charles (✉)
Equideum Health, Denver, CO, USA

University of Colorado Denver, Business School, Denver, CO, USA

University of Denver, Denver, CO, USA
e-mail: wendy.charles@cuanschutz.edu

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_3

consent generally focus on respecting an individual's choice and protecting that individual's freedom to provide, change, or revoke permissions (Asghar & Russello, 2012). As an example, the General Data Protection Regulation defines informed consent as including the following characteristics: being unambiguous, informed, freely given, specific, auditable, explicit, and with the capability of withdrawal ("General Data Protection Regulation," 2016).

For an individual's participation in a research study, informed consent is both a legal and ethical requirement (21 CFR § 50, 2013; 45 CFR § 46, 2018; *WMA Declaration of Helsinki—ethical principles for medical research involving human subjects: Adopted by the 64th WMA General Assembly, Fortaleza, Brazil*, 2013). Human research protection regulations and guidance documents describe informed consent as a voluntary, affirmative decision where concise information is presented in sufficient detail such that the key concepts could influence an informed decision (21 CFR § 50, 2013; 45 CFR § 46, 2018; International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use, 2016). Further, information cannot involve exculpatory language, coercion, or undue enticement (Department of Health and Human Services, 2011). Of most significant consideration, informed consent is not a document but a *process*, beginning with the first recruitment initiative until study completion (Office for Human Research Protections, 2016).

As consent is sought for long-term initiatives, such as research databases and biobanks, organizations must determine how to maintain the consent process throughout participation. This chapter explores why the standard methods of obtaining informed consent are insufficient to maintain the consent process and why blockchain-based dynamic consent mechanisms promote more ethical and efficient methods of ongoing consent.

While there are many settings where blockchain-based dynamic consent can be deployed, it was necessary to narrow the scope of this chapter due to space limitations. First, this chapter focuses on dynamic consent for managing health-oriented research data because individuals tend to have different research preferences for health data than non-health data (Ploug & Holm, 2016). Next, this chapter recognizes that certain forms of health research can be conducted under an Institutional Review Board (IRB)-issued a waiver of informed consent, a partial waiver of informed consent, or a waiver of documentation of informed consent (45 CFR § 46.116–117). However, to illustrate concepts of blockchain-based dynamic consent, this chapter focuses only on the circumstances where an individual would provide affirmative and explicit written informed consent. Last, considering the vast number of international regulatory requirements for health-related research, this chapter focuses primarily on U.S. regulations with occasional mentions of other countries or regions.

2 Current Drawbacks of Traditional Informed Consent

While researchers routinely request informed consent when an individual is approached for participation in a research study, there is growing interest in collecting data and specimens that could be used for future "secondary" research. To maintain long-term storage, data management strategies can involve databases (e.g., recruitment databases), data/specimen repositories, biobanks, or other similar mechanisms that involve curated data and/or specimens. (While each of these data and storage mechanisms has unique features, they will be referred to henceforth collectively as "research repositories.") Under other circumstances, data or specimens could be provided—or even sold—to other researchers (Charles & Delgado, 2022b). Organizations often provide administrative support to manage research repositories for multiple researchers and projects (Cheung, 2018).

Because risk is inherent with the collection and storage of data and/or specimens for future research use, organizations that maintain data and/or specimens are encouraged to obtain ethical research oversight and obtain informed consent from participants whenever possible (*WMA Declaration of Taipei on ethical considerations regarding health databases and biobanks: Revised by the 67th WMA General Assembly, Taipei, Taiwan, October,* 2016). As a result, many researchers obtain individuals' informed consent for participation in a research repository with consideration that they could not anticipate the complete nature of future research that could be conducted. Therefore, individuals are asked to provide consent based on basic descriptions of the types of future research that could be conducted without providing informed consent for each subsequent use of their data or specimens (Office for Human Research Protections, 2017).

2.1 Consent Strategies

2.1.1 Broad Consent

One mechanism to obtain open-ended informed consent for future research involves "broad consent." Broad consent has long been used to describe requesting permission for a broad range of future data sharing or research options that have not yet been designed or determined (Cheah et al., 2018). As a common approach for asking for data or specimens to be stored in a repository, the permissions could be unlimited (e.g., "for medical research") or could be limited to a specific area of research (e.g., "for Cardiology research") (Appenzeller et al., 2022; Leon-Sanz, 2019). The strategy is to provide as much information as possible at the time of consent and customize the scope of details based on the organization's projects and goals (Appenzeller et al., 2022). Researchers who wish to obtain identifiable data and/or specimens from research repositories must pursue the appropriate regulatory oversight within their institution or jurisdiction (Leon-Sanz, 2019). The nature of this type of broad consent is generally acceptable by regulatory authorities in many countries (Rothstein et al., 2018).

While most organizations describe the concept of broad consent in a generic sense, the U.S. Department of Health and Human Services, along with 15 other U.S. Federal Agencies, revised the regulations for the Protection of Human Research Subjects in Research in 2018 (i.e., "The Common Rule"; 45 CFR § 46, 2018). The Common Rule now offers a formal framework and definition for broad consent codified in 45 CFR § 46 and described in guidance documents (Office for Human Research Protections, 2017). The regulation creates a category of permissible secondary research involving broad consent for storage, maintenance, and use in future research. The new parameters of "Common Rule broad consent" differ from unlimited or blanket consent options when managing a person's refusal to provide broad consent. Specifically, if an individual is asked to provide broad consent subject to the Common Rule (45 CFR § 46, 2018), and the individual refuses to consent for all or part of the future research, the IRB cannot waive the requirements for consent for the use of identifiable private information or specimens and the person's wishes must be honored (45 CFR § 46.116(f), 2018).

Drawbacks

After providing broad consent, individuals are generally not asked for informed consent again—or typically even notified when their data or specimens are used or shared in the future. Therefore, ethicists have questioned whether such an open-ended consent strategy is truly ethical (e.g., Cheah et al., 2018; Dulhanty, 2021; Wee, 2013). Additionally, the nature of a broad consent process restricts an individual's autonomy (Mamo et al., 2019) in a few fundamental ways:

1. A one-time broad consent process is often presented with a *take-it-or-leave-it approach*. Individuals may be asked to consent to all future research or broad categories of research without an opportunity to object to specific types of research they may find objectionable (Alhajri et al., 2022). For example, a person may be asked to consent to future Immunology research but may have a personal objection to genomic research methodology that could be used within Immunology research. Therefore, an individual who would like to contribute to future research must agree with the consent form (or category of research) in its entirety or be denied the opportunity to contribute to future research.
2. *The nature of future research is unknown* at the time of consent. Cheah et al. (2018) argue that individuals cannot provide valid informed consent if they do not know how their identifiable data or specimens will be used in the future. As examples:
   (a) Since biobanks may store specimens for many years, *new types of research will be invented* that the individual could not have anticipated at the time of consent (Mamo et al., 2019). It is then unknown whether an individual may find some of these types of research objectionable.
   (b) *New risks may emerge in future research*. This issue is particularly problematic regarding advances in genetic research that do not simply create information risks for the individual but for the individual's blood relatives (Gibbons et al., 2007). Additionally, with rapid advances in big data and

data linking, new risks from reidentification may emerge (Rupasinghe et al., 2019).

(c) *A person's preferences may change over time*. As people engage with news about medical research and experience new life events, their stated preferences during the initial consent process could become outdated and may no longer reflect their preferences (Custers, 2016).

While there are mechanisms by which individuals could contact the researcher and/or administrator to request changes or withdrawal from research, such processes are typically manual and effortful (Kaye et al., 2015). Further, Leon-Sanz (2019) notes that many individuals would prefer to be contacted and asked for permission for subsequent uses.

2.1.2 Meta Consent

A similar and overlapping approach to a broad consent process involves "meta consent." Individuals could be offered choices about how and when they prefer to be contacted for future research (Ploug & Holm, 2016). With this approach, meta consent processes are designed to manage and configure individuals' preferences to be contacted for permission regarding specific types of data, researchers, research settings, or study aims (Cheung, 2018). A meta consent process triggers future outreach, intending to respect a person's values and vulnerabilities (Ploug & Holm, 2016).

Regardless of the consent methods described above, it is challenging to maintain informed consent for future sharing and use in an efficient, customizable, and transparent method (Kakarlapudi & Mahmoud, 2021). Of most significant importance, Tith et al. (2020) note that when it is difficult for individuals to change their data and/or specimen-sharing decisions, they are reluctant to agree to participate in future health research. Therefore, researchers are increasingly utilizing methods of dynamic consent to engage individuals in their consent preferences over time.

2.2 Dynamic Consent

2.2.1 Definition

Dynamic consent is often described as a flexible, configurable, electronic consent (e-consent) design that can more easily capture an individual's consent preferences across a spectrum of choices over time (Budin-Ljøsne et al., 2017; Kaye et al., 2015). In contrast with a passive traditional paper-based broad consent mechanism, the informed consent process is "dynamic" because an individual can alter or withdraw consent choices after receiving new information or responding to changing circumstances (Kaye et al., 2015).

Additionally, dynamic consent management utilizes an electronic platform. An interactive user interface allows individuals to engage with their information choices using a smartphone, tablet, or computer for easy access and immediate modifications

without the need to contact researchers or administrators to request changes (Leon-Sanz, 2019). Similarly, a dynamic consent platform can more easily offer a communication system for an interactive flow of information between stakeholders (Appenzeller et al., 2022). Further, an audit trail captures an individual's changes for verification (21 CFR § 11.10(e); Mamo et al., 2019). Overall, the primary goal of dynamic consent is to allow an individual to remain engaged in an ongoing consent process.

2.3 Benefits of Dynamic Consent

In addition to the benefits of electronic consent technology that reduces the likelihood of missed pages, consent form storage, and version control, dynamic consent addresses the need for informed consent to be an *ongoing process*, not a one-time event (Benchoufi et al., 2018). Dynamic consent offers a participant-centered technology with several ethical and practical benefits.

2.3.1 Rights

First and foremost, an individual's autonomy to make informed decisions should not be passive or static. Fundamental to an informed consent process, "respect for persons" suggests that individuals should be given as much information and choice as is feasible for the duration that their identifiable data and/or specimens could be used (Taylor & Whitton, 2020). This autonomy is further enabled by allowing an individual to interact with new information or consult others in an unpressured context; the individual can then provide more meaningful consent (Kaye et al., 2015). Leon-Sanz (2019) suggests that a continuous consent process obtains a person's permission while respecting the person's changing values.

2.3.2 Recruitment

An additional purported benefit of dynamic consent for researchers is that dynamic data management systems provide extensive data for researchers to identify prospective participants for future studies. Dynamic consent software can allow data to be queried for updated demographics, health conditions, and even levels of system engagement to identify individuals who may agree to participate in new research (Kaye et al., 2015). In addition to finding prospective research participants, the nature of the data makes the recruitment process less administratively burdensome and costly (Kaye et al., 2015). Some researchers may also reach out to individuals who have agreed to future contact to seek advice about protocol designs or possible community recruitment methods (Budin-Ljøsne et al., 2017).

2.3.3 Control

Chalil Madathil et al. (2013) demonstrated that individuals prefer more control over how their health information is used in research. Therefore, dynamic consent platforms allow organizations to refine consent options more granularly than an all-or-nothing approach. In this manner, individuals could be presented with several

choices regarding how their data and/or specimens are used (Budin-Ljøsne et al., 2017), for the duration of time consent could be granted (Kaye et al., 2015), and/or whether the future use may include genetic research (Mamo et al., 2019). Specifically, most individuals whose specimens could be used for genomic research would prefer to be asked prior to use (Robinson et al., 2013).

Dynamic consent capabilities also enable individuals to permit which organization or researcher can gain access to their data (Agbo & Mahmoud, 2020). Patients customarily grant permission to their physicians but could extend the permissions to others, depending on the perceived level of trust (Jacobs, 2021). Similarly, individuals may wish to share only with non-profit organizations (Chen et al., 2020) or specify the duration or nature of permitted uses of data (Agbo & Mahmoud, 2020). Most dynamic consent platforms allow an individual to change researcher access permissions at any time (Budin-Ljøsne et al., 2017).

As described above, there are circumstances where an individual's preferences could change, and there should be a mechanism for ongoing interactions between researchers and participants (Custers, 2016). Similarly, individuals may wish to take a break from research for a period, and the dynamic consent interface could allow for a simple and straightforward mechanism to communicate the change (Kaye et al., 2015).

While dynamic consent permits individuals to change their permissions, it should be noted that individuals' requests to withdraw permission for uses of their data and/or specimens apply only to future uses of their identifiable data and/or specimens. Modifications or withdrawals do not apply to data and/or specimens already used in research (Mamo et al., 2019). As an additional option, individuals may request that identifiable information be removed from their data, permitting future use of de-identified data and/or specimens.

2.3.4 Communication

Standard, one-time informed consent practices usually involve interpersonal interactions between researchers and prospective research participants. On the other hand, dynamic consent interfaces provide an electronic user interface that expands beyond the traditional one-time consent process for more communication over time (Kaye et al., 2015). Specifically, these interactions could involve text messages, secure messages, online forums, chat rooms, webinars, or teleconference visits (Budin-Ljøsne et al., 2017). Researchers could provide updates about the research studies, describe new research opportunities, or request that the individuals update their health or contact information (Kaye et al., 2015).

Dynamic consent systems can also address individuals' interest in learning about their own research participation. According to Blasimme et al. (2017), 78% of research participants are interested in receiving information about their own lab and test results at the end of the study, with a preference for receiving recommendations for follow-up care. Blasimme et al. (2017) argue that it is morally objectionable for researchers to withhold (non-blinded) clinically actionable information collected about individuals for a research study. Instead, communicating these results is necessary to ensure the individuals' ongoing health and well-being.

The improved communication offered by dynamic consent platforms also can extend research participation to populations that may normally encounter barriers to traditional research participation, such as geographic distance or physical inability (Brall et al., 2019), and could enable population-based research (Budin-Ljøsne et al., 2017).

2.3.5 Engagement

Kaye et al. (2015) describe the nature of dynamic consent engagement as a "partnership" where individuals are more likely to agree to future research and express more trust in the research. The enhanced collaboration can also enable the creation of connected communities who share a health condition and can support each other in future research (Avdoshin & Pesotskaya, 2018). Ultimately, increased engagement results in a more informed research population with more awareness regarding how data and/or specimens are used and processed to advance research (Custers, 2016).

2.3.6 Resources

Utilizing electronic documentation and communication may reduce research costs in the long run (Kaye et al., 2015). Researchers who rely on paper consent forms describe the cumbersome task of printing, copying, and scanning consent forms (Chalil Madathil et al., 2013). Additional efficiencies result from the reduced need for research staff to perform data entry about an individual's preferences because an individual enters preferences into the system directly (Despotou et al., 2020). Additional savings could involve reduced costs of paper, printing, storage, quality review controls, and automation for pushing new information to individuals electronically instead of by manual efforts of letters or individual emails (Brall et al., 2019; Budin-Ljøsne et al., 2017).

2.4 Regulations

While some research regulations were described earlier, a complete description of country-by-country health information and privacy regulations for electronic or dynamic consent is outside the scope of this chapter. For a detailed review of international digital and dynamic consent comparisons, the reader is encouraged to review DeSutter et al. (2022), "Digitizing the informed consent process: A review of the regulatory landscape in the European Union." In summary, the requirement to document individuals' electronic signatures varies, depending on the applicable regulations (Asghar & Russello, 2012). For example, the Uniform Electronic Transactions Act specifies that an electronic signature has the same validity and enforceability as a written signature as enacted by (National Conference of Commissioners on Uniform State Laws, 1999) and the Electronic Signatures in Global and National Commerce Act ("Electronic Signatures in Global and National Commerce Act," 2000). There are many mechanisms by which an individual can provide an electronic "signature," such as clicking a box, toggling switches, typing one's name, recording one's voice, or signing one's name with a stylus or mouse

(Anabo et al., 2019; Charles et al., 2019). For research regulated by agencies entrusted with drug, biologics, and device safety, there may be more stringent requirements to ensure the integrity of a digital signature (European Medicines Agency, 2022; U.S. Food and Drug Administration, 2017).

3 Limitations of Traditional Dynamic Consent

While dynamic consent aims to include individuals as partners in the decision-making process, some technological drawbacks should not be overlooked.

While dynamic consent technology is improving, centralized systems face several challenges. First, managing a large repository's access is quite resource-intensive. Datasets are often administratively curated to ensure that a researcher receives only the data individuals have provided consent for, requiring high costs and administrative demands (Budin-Ljøsne et al., 2017). Even when data are carefully curated, it may be impossible for a database owner to prevent a researcher from conducting different or subsequent analyses outside the proposed research (Taylor & Whitton, 2020). Further, there are often insufficient resources to provide Help Desk support for individuals or researchers with questions or concerns (Kaye et al., 2015). Last, it is unclear what would happen with individually-identifiable data and/or specimens if the repository goes out of business or changes its business practices (Agarwal et al., 2020).

With consideration of technological limitations, many electronic databases do not have an audit trail to track access to the data or the ability to determine if there was inappropriate access or use (Rupasinghe et al., 2019). Moreover, centralized architecture may force unified and logical structures for the data models, losing or limiting the nature of contextualized data available for interpretation and analysis (Shrestha et al., 2020). Among these data limitations, traditional dynamic consent software may not allow individuals to customize their sharing preferences or delegate consent rights, limiting them to the categories chosen by the research organization (Merlec et al., 2021). In addition, the dynamic consent solution may have interoperability limitations with other software intended to receive and subsequently manage the data (Albalwy et al., 2021).

Similarly, technology maintained on a central server could be vulnerable to disruptions, ransomware, breaches, and data manipulation (Shrestha et al., 2020). These technological limitations create concerns about ongoing accountability, security, and transparency of operations (Merlec et al., 2021). Specifically, the database is still vulnerable to privacy and security breaches that can create varying levels of risk for identifiable information (Kaye et al., 2015). Overall, individuals must then trust the organization's integrity instead of its technology (Alhajri et al., 2022).

4 Why Blockchain?

Blockchain-based technology for managing dynamic consent provides features that allow more capability for dynamic consent and can augment the capabilities and workflow of existing systems (Jung & Pfister, 2020). Generally, dynamic consent systems that include blockchain tools and technologies may offer more flexibility, integrity, and accountability than traditional data systems (Albalwy et al., 2021).

4.1 Smart Contracts

Blockchain-based smart contracts involve small segments of code that are algorithmically implemented to execute when specific conditions are met (Chamber of Digital Commerce, 2018). As a software layer integrated with a blockchain, smart contracts are tamper-resistant and tamper-evident and can only be modified by subsequently updated specifications (Agbo & Mahmoud, 2020). Smart contracts enhance access capabilities in the following ways:

1. Rather than limit access to role-based access controls customary in many traditional software systems, smart contracts allow for *granular access management*. For example, individuals could specify data sharing to include a single individual or a group of researchers or institutions. Similarly, smart contracts can expressly exclude individuals or groups at a granular level (Agarwal et al., 2020). Participants can also share their data with the public domain outside of the research organization that manages the data (Cheung, 2018). A research participant can set, modify, revoke, or set these permissions to expire at any time.
2. The granular access controls also *extend permissions to specific data variables*. Individual variables can be expressly included or excluded from data sharing, and these selections can be modified, revoked, or set to expire at any time (Velmovitsky et al., 2020). Specifically, for certain types of research, individuals express concern about sharing GPS locations or sensitive health information with researchers (Cheah et al., 2018).

Smart contracts also automate many features and data flow that may have otherwise been manually administered.

1. A researcher-facing user interface can *allow researchers to perform their own queries* of available research data. Smart contracts limit visibility and access to data unless a participant (and sometimes an administrator) has granted permission (Cheung, 2018). This feature reduces the administrative burden of curating and verifying that a data set is honoring individuals' preferences and terms for future use of their data. This feature could be further enhanced by requiring evidence of IRB review before releasing identifiable information.
2. Smart contracts can *automate data flow between processes or systems*. For example, if an individual agrees to additional terms of a research study, the

randomization event could execute a smart contract to update supply management (Learney, 2019).

3. Smart contracts can *apply schemas to data to allow for semantic interoperability*. For example, when combining data sets, smart contracts can be specified for a study to allow for temporary variable and/or value recoding to match variables and/or values across data sets (Shrestha et al., 2020). While this practice can also be achieved using statistics and data science, smart contract schemas are often desirable for efficiency (Charles, 2021a).
4. Smart contracts can *issue alerts* to research participants, research personnel, or safety monitors when data (or trends) exceed a defined limit (Jung & Pfister, 2020).
5. Smart contracts are also used to *manage layers of governance and oversight*. For example, smart contracts can enforce specific data-sharing limitations, such as preventing researchers from sharing data outside their institutions or preventing private health information from being shared outside national boundaries (Charles, 2021a).
6. As individuals seek greater transparency and access to their own information, smart contracts *can prevent individuals from accessing certain information*, such as single- or double-blinded test results that could be legally withheld under federal regulation or state statutes (Charles, 2021b). Blinded health data could be automatically released to an individual at the end of his or her participation (Porsdam Mann et al., 2021).
7. Blockchain-based smart contracts are also increasingly used to *provide monetization to individuals* to recognize that their data has been accessed by researchers or other data enterprises (Charles & Delgado, 2022a). For example, emerging blockchain-based data marketplaces use smart contracts to automate individual payments (Spanò et al., 2021).

4.2 Audit Trails

As data are added to and accessed from blockchain-based research repositories, the audit trail inherent in blockchains captures changes an individual has made to their preferences and can also capture researchers' access to data sets. For specific benefits:

1. Research participants could *examine the audit trail* to see who has accessed their personal information, allowing for more visibility into the research process (Agarwal et al., 2020). This technology can also allow an individual to examine both identifiable and anonymized data releases (Calvaresi et al., 2019).
2. Researchers' and administrators' *access could be tracked and managed* on the blockchain, holding these roles accountable (Mamo et al., 2019). Tracking researcher access on a more granular level also makes it possible to trace the value resulting from publications and grants (Porsdam Mann et al., 2021).

3. Blockchain-based audit trails also allow a more efficient mechanism to *track data provenance* from the point of data collection through access and movement through data systems (Jung & Pfister, 2020).
4. *Compliance staff or regulatory agencies* could examine this audit trail when *evaluating data access and quality* (Learney, 2019). Because a blockchain-based audit trail can capture end-to-end data use, the audit review process could cover data collection and processing through analysis (Jung & Pfister, 2020).

4.3 Smart Data

When capturing metadata and/or raw data on a ledger instead of a flat data table, it is possible to capture deep contextualization of the data. For example, when an individual provides dynamic consent, it is possible to capture additional attributes associated with the consent process (Rupasinghe et al., 2019). This contextualization can include the nature of authorized operations, the permitted context for research, creation time, storage location, relationships, and the validity period (Rupasinghe et al., 2019). Additional attributes can include data ownership (i.e., custodianship and/or control) for more robust access management (Agbo & Mahmoud, 2020; Charles, 2021c). The smart data components can also create portable permission structures that individuals can maintain with their data instead of with the organization (Cheung, 2018). Similarly, data ownership and control can be maintained by the individual in the same way as an organ donation card (Cheung, 2018).

4.4 Architecture

Blockchain-based dynamic consent is based on controls that can impart more data security. First, physical and logical storage decentralization offers stronger protections than centralized databases that involve only a single point of failure (Albalwy et al., 2021). Also, the cryptography used with blockchain-based systems can offer stronger data security (Albanese et al., 2020). Last, data security can be enhanced with other privacy-preserving cryptography features, such as zero-knowledge proofs or homomorphic encryption (Learney, 2019; Merlec et al., 2021).

4.5 Examples

Several blockchain-based dynamic consent software programs have been proposed and are in various stages of commercialization. The following is a sample of named technology solutions for illustration purposes without promotion. Any inaccuracy or omission of other technologies is unintentional.

ADvoCATE is a blockchain-based dynamic consent management tool designed to address privacy protections for IoT devices (Rantos et al., 2019). The consent

management component automates individuals' personal data preferences into rules. Blockchain technology offers non-repudiation and versioning.

ConsentChain is proposed as a blockchain-based consent system to dynamically share patients' genomes (Albalwy et al., 2021). Data are managed with hybrid off-chain/on-chain storage where the reference pointer to off-chain storage is encrypted for security.

Consentio manages consent dynamically by separating the consent management layer from the data management layer (Agarwal et al., 2020). Electronic health records remain stored in an off-chain health record database, while blockchain-based audit trails track permissions and health record access.

CrowdMed is introduced as a blockchain-based dynamic consent solution for sharing healthcare data with healthcare providers (Shah et al., 2019). CrowdMed offers granular consent options, while the blockchain maintains consent contracts and can provide incentives when individuals share data for research. The technology can be integrated with existing data systems.

The *Dovetail* network is designed to enable patients to exchange health information with care providers (Despotou et al., 2020). Dovetail does not access or manage health data but facilitates dynamic consent and tracks the anonymized details of the exchange on the ledger.

D-CSCM is proposed as a blockchain-based decentralized clinical study consent management solution (Jung & Pfister, 2020). Smart contracts create and manage consent permissions, while consent forms are maintained with decentralized storage. The blockchain logs all views and modifications to the database and consent forms.

Dwarna is a web portal to allow patients to provide dynamic consent for a biobank (Mamo et al., 2019). The blockchain pseudonymizes individuals' identities and acts as a hub to connect patients with researchers.

DynamiChain is proposed as a medical blockchain-based medical network to manage dynamic data sharing using rules management algorithms (Kim et al., 2021). The blockchain synchronizes smart contracts and tracks stakeholder access with hash functions.

EnCoRe offers a dynamic consent management layer to allow individuals to manage data sharing with enhanced privacy (Merlec et al., 2021). The consortium network allows secure data exchanges among stakeholders with transparent tracking on a blockchain.

LifeGraph is a blockchain platform that offers a dynamic consent and governance layers to unify and share data at scale (Hartley, 2022). Using graph databases for longitudinal data management, disparate data sources can be linked to create hyper-personalized insights.

LUCE is proposed as a dynamic consent model that allows both data providers and requesters to interact with a blockchain-based platform (Jaiman & Urovi, 2020). Patients can specify and dynamically change their permissions, while data requesters can perform data queries without an administrator. The Ethereum blockchain facilitates smart contracts and auditability.

MedRec is among the first blockchain-based consent management systems that allow patients to own health data and manage data viewership permissions (Azaria et al., 2016). The blockchain stores and displays consent details.

METORY is a blockchain-based dynamic consent platform designed for clinical trials (Huh et al., 2022). The blockchain's hash values (and corresponding QR codes) demonstrate consent form integrity, while the blockchain also manages access controls and data security.

SCoDES is intended to provide dynamic and decentralized consent management for clinical trials (Albanese et al., 2020). The blockchain offers distributed storage and connections to medical platforms with traceability and trust.

4.6 Summary

This section shared how blockchain-based dynamic consent offers several advantages over centralized consent management; however, this chapter recognizes that traditional software applications could be designed to offer some of the features inherent in blockchain tools and technologies. The primary difference appears to be the prevalence of "trust" described among blockchain-based solutions. Consistent themes within the blockchain-based systems involve descriptions of data visibility (Kakarlapudi & Mahmoud, 2021) with transparent governance procedures (Mamo et al., 2019). Velmovitsky et al. (2020) note that many blockchain-based dynamic consent systems are developed to identify and mitigate trust issues in a consent process. Individuals who are offered dynamic choices and visibility into how their choices are honored are more likely to trust the researchers and agree to participate in research (Schuler Scott et al., 2019).

5 Remaining Concerns and Recommendations

While blockchain can offer many positive features toward dynamic consent management, issues remain that should be considered and addressed to optimize dynamic consent for data sharing and research.

5.1 Need for Digitization

The first consideration regarding dynamic consent requires that technologies are available to capture consent from individuals in an electronic format. While some paper-based consent forms could be entered into an electronic database system to record and manage a person's consent preferences, this process does not offer dynamic interactions for ongoing consent management (Appenzeller et al., 2022). As noted earlier, scanning paper consent forms and/or performing manual data entry is a time-intensive process that is unlikely to be cost-effective (Albanese et al.,

2020). The degree to which digitized data are available will strongly influence the value proposition of blockchain-based dynamic consent mechanisms.

5.2 Scientific Design

Blockchain-based dynamic consent solutions aim to empower patients with more control over the access and use of their health information. While this is a decisive advance toward individual autonomy, there could be repercussions for scientific research designs and integrity. Specifically, when individuals must "opt in" to share their health data (or restrict access to some or all data within a health or research setting), there is a substantial risk of selection bias that could strongly skew the patient population available for study (Porsdam Mann et al., 2021). As an additional concern regarding selection bias, Chen et al. (2020) relay that individuals who use electronic technologies to enroll in biorepositories are less demographically and ethnically diverse than individuals who enroll with paper-based consent. Therefore, to mitigate selection bias, organizations should deliberately recruit individuals who tend to be underrepresented in clinical research and craft strategies for ongoing retention (Rahimzadeh, 2021).

5.3 Digital Design

When designing blockchain technology for any dynamic consent software solution, there are considerable differences between blockchain platforms' strengths and weaknesses. The blockchain could store the data on-chain, off-chain, or hybrid storage systems with varying levels of encryption and security (Kakarlapudi & Mahmoud, 2021). Depending on the platform and API integrations, there could be security vulnerabilities within the blockchain (Albalwy et al., 2021) or smart contracts (Destefanis et al., 2018). For example, smart contract security audits should be conducted on an initial and ongoing basis to ensure that smart contracts operate as intended (Albalwy et al., 2021).

5.3.1 Interoperability

A primary challenge when establishing data-sharing mechanisms across health and research settings involves the interoperability of disparate systems. While there is increasing adoption of Fast Healthcare Interoperability Resources (FHIR using HL7 standards), these are not yet widely used among consent management solutions to integrate with existing healthcare or research technologies (Appenzeller et al., 2022) or with blockchain technologies (Kakarlapudi & Mahmoud, 2021). Further, many existing health information technologies are not designed to allow individuals to see who has accessed their health information or to allow individuals to control access (Despotou et al., 2020). Therefore, blockchains may be prevented from tracking data access across certain data systems—particularly legacy systems. Incompatibility may also be semantic, involving different data and privacy ontologies, which may

reduce data matching when datasets use non-standardized variable naming (Rantos et al., 2019). Mitigating these incompatibilities may require significant advanced planning regarding data ontologies and system architecture (Rupasinghe et al., 2019).

5.3.2 Privacy and Security

Privacy is often defined as individuals' ability to manage the collecting, sharing, and processing of information about them (Alhajri et al., 2022). Alhajri et al. (2022) note that individuals strongly consider their health data privacy when deciding to share their data. Among privacy considerations, many dynamic consent databases maintain a link to the individuals' identities so that health and other pertinent information can be updated (Mamo et al., 2019). Also, biospecimens only offer meaningful study outcomes when linked to pertinent health or lifestyle information (Mamo et al., 2019).

The nature of privacy protection depends on the degree to which the information is subject to health or research regulations and the jurisdiction in which the database or participants are located (Ballantyne, 2020). Generally, there should be strong privacy policies and controls to ensure that an individual's identifiable information is not inappropriately accessed or released.

The growing prospect that individuals' de-identified data could be combined with other sources to reveal their identities raises additional questions about how the data or system capabilities could be designed to respect individuals' privacy. Strategies for releasing only de-identified information are not fool-proof, and it is increasingly feasible to link data with other sources (Cheung, 2018).

Provisions for data security often reside within systems' software, architecture, and maintenance (Chia et al., 2018). Organizations can review the possible security risks by conducting a thorough technological and operational risk assessment (Bhushan et al., 2021). The nature of risk assessment could involve assessing procedures for data handling, methods of data transmission, the number and nature of variables released, and internal training (Cheung, 2018). The risk assessment should also involve external penetration testing and code review. These security assessments should be conducted regularly to recognize emerging threats and risks (Cheung, 2018).

Because there can be blockchain design flaws (Chia et al., 2018), information about confidentiality provided to research participants should not provide a false sense of security or overstate the privacy of their information (Appenzeller et al., 2022). Cheung (2018) notes that some scholars recommend an approach involving "radical honesty" during the repository enrollment process about the potential risks of breaches and risks of reidentification.

Last, irrespective of security and release methods, protecting individuals' identifiable information may also rest with the researchers receiving the data. If not already under a contractual or regulatory responsibility, researchers can be asked to sign agreements that they will not attempt to re-identify data or share data with other individuals or organizations (Cheung, 2018). Researchers could also be required to

follow organizational policies and procedures, including technology best practices (Lacity & Khan, 2019).

5.3.3 Key Management and Identity

When designing access management for a blockchain-based dynamic consent solution, it is critical to consider how the user's identity will be verified and whether identity management services will be centralized to the organization administering the technology. As noted above, an electronic signature involves legal implications that the person signing the document(s) has the legal authority to do so ("Electronic Signatures in Global and National Commerce Act," 2000). If involving health information, only the patient or legally authorized representative has the right to share the patient's health information (Office for Civil Rights, 2008). Further, if patients could be minors, the organization may be required to transition decision-making authority to the child-turned-adult when the individual reaches the age of majority in his/her jurisdiction (Leon-Sanz, 2019).

Blockchain-based system access is managed with private and public key pairs. However, it is difficult for patients to manage passwords—much the less long hash strings—and keys must be recoverable in the event of accidental loss (Verde et al., 2019). Therefore, blockchain vendors have progressed toward more user-friendly mechanisms for storing and recovering keys (Learney, 2019). Emerging methods offer key management schemes that associate blockchain keys with passwords or single sign-on mechanisms (Merlec et al., 2021), while other organizations may choose to use a trusted agency or administrator to manage access (Verde et al., 2019).

A thorough description of blockchain and smart contract design features is outside the scope of this chapter. However, readers are encouraged to consider the impact of different blockchain design choices on dynamic consent system cost, privacy, and security.

5.3.4 Regulatory Requirements

Depending on the dynamic consent system's interactions with healthcare or research organizations, it may be necessary to build regulatory requirements into the technology and organizational operations. To receive information from healthcare organizations or providers in the USA, research repositories may have to agree to terms as Business Associates and implement physical, administrative, and technical safeguards (45 CFR § 164). If managing data that may be processed and used as part of an application to a regulatory agency, it may be necessary to meet technical and procedural controls required by the FDA or EMA (Charles, 2022; Charles et al., 2019). Therefore, it is critical to determine how data will be received and used to ensure that regulatory requirements will be met.

5.4 Ethical Considerations

To address individuals' questions and needs throughout research repository participation, organizations should anticipate and proactively address issues pertaining to ethical design and interactions with individuals. Nearly all of the following considerations pertain to the components of dynamic consent instead of blockchain technologies.

5.4.1 Can Individuals Access the Technology?

When designing technologies used by patients or a broad range of users, it is necessary to consider the planned populations' potential technological limitations. First, there are concerns about whether the planned participants will have sufficient access to broadband technologies, which can be influenced by geography, age, socioeconomic status, and housing stability (Kaye et al., 2015). Similarly, not all individuals may have sufficient access to smart technology, such as a computer, tablet, or smartphone, that would allow them to connect to dynamic consent applications to manage their preferences (Brall et al., 2019; Charles & Magtanong, 2022). Specifically, residents of rural communities and individuals within minority populations have expressed concern regarding access to the Internet to utilize electronic consent technologies (Chen et al., 2020).

5.4.2 Is Consent Informed?

The premise behind dynamic consent technology is informed consent, but organizations may not realize the limitations of an individual's comprehension. Simply providing information and encouraging individuals to make choices does not mean that their choices are informed (Cheung, 2018). Because individuals possess different health and technology literacy levels, they may be unable to understand and assess their options to make informed decisions (Ballantyne, 2020). Cheah et al. (2018) note that many research participants do not understand the comprehensiveness of the terms "data" and "sharing" within a research context. Community members—including some researchers—may not have previous experience using data and/or specimens for secondary research and are unfamiliar with research oversight and protection requirements (Cheah et al., 2018).

When contemplating whether individuals are making informed choices, it is also worthwhile to consider individual behaviors during the consenting process. For example, there is often a contradiction between individuals' stated interests in data protection and their actual behaviors, referred to as the "privacy paradox" (Muravyeva et al., 2020). Specifically, individuals may exhibit "habituation" when interacting with electronic consent forms. Habituated consent involves blindly accepting agreements without reading the privacy terms or selecting among available options (Muravyeva et al., 2020). Custers (2016) speculates that habituation worsens when web-based agreements are presented as all-or-nothing/take-it-or-leave-it non-negotiable terms and individuals become trained to simply "agree." Therefore, the degree to which a consent process is "informed" often depends on the

degree to which the intended population is knowledgeable, competent, and/or engaged when using a dynamic consent system.

5.4.3 Should Results Be Shared?

Because some dynamic consent applications advertise that they can provide clinical and/or research results back to research participants, providing this information requires advanced planning and communication strategies. For example, laboratory testing of blood specimens could yield clinically actionable findings, and genetic testing could reveal predispositions to disease (Blasimme et al., 2017). As noted earlier, the findings from genetic information are particularly sensitive because they do not just affect the research participant but may also create questions and concerns from blood relatives (Gibbons et al., 2007). Therefore, organizations that plan to provide individual results to research participants should consider how the information will be presented and whether clinical interpretations and support will be available.

5.4.4 Possible Strategies

While there are no clear solutions to the considerations listed above, there are methods organizations can consider or implement to reduce the impact. Brall et al. (2019) recommend an "ethics by design" approach to reduce barriers to individuals' participation and/or comprehension. These may include the following:

Technology Features

1. Dynamic consent user interfaces should be designed to be easily viewed and navigated on smartphones to promote access for individuals who lack other computing devices (Kaye et al., 2015). Ideally, there should be fewer images to allow individuals with slower bandwidth speed to complete their desired interactions with the app.
2. The design features should be determined by interacting with the planned population or community that will use the dynamic consent technology. Often conducted in focus groups, representative individuals should provide feedback on the nature of the information that needs to be communicated, such as why they should participate in data sharing and how they should view concepts of privacy. Such focus groups are essential when there are plans to include individuals from indigenous communities who may find the concept of individually-owned and controlled health data incompatible with the perspective that these are shared community resources (Rahimzadeh, 2021).

Ensure an Ongoing Consent Process

3. When individuals are presented with dynamic consent technology, instruction and assistance should be available to ensure they can navigate the app and understand the meanings behind their choices. It is also vital for individuals to receive accurate information about informational risks and risks of

reidentification, as well as best practices for device security. It may not be necessary to explain that blockchain is involved so long as the information describes system security, transparency, and auditability (Charles, 2021a).

4. To ensure that dynamic consent is genuinely "informed":
   (a) Individuals' comprehension can be assessed with electronic "quiz" questions during the initial presentation of the dynamic consent solution or can be assessed periodically with "knowledge checks" within the user interface (Barrera et al., 2016).
   (b) There should be ongoing communication within the dynamic consent app to ensure that individuals have sufficient information to inform their consent choices. Such communication may involve summaries of new research findings, highlights of new disease recommendations, or software updates to the platform.
5. To achieve a truly "dynamic" interaction with the technology, individuals must remain engaged throughout their involvement. Engagement could come from researcher outreach and through gamification strategies to reward interactions, such as points, badges, and push-message reminders (Kaye et al., 2015).
6. The process of dynamic consent should not eliminate the potential interactions with researchers or staff (Kaye et al., 2015). While many questions could be answered through an initial consent process and frequently asked questions pages within the user interface, there should still be a mechanism by which a patient or research participant can engage with a human being if there are questions or needs for help (Rahimzadeh, 2021).

Communication

If the plan is to provide research results back to individual participants, Blasimme et al. (2017) recommend that organizations develop procedures for the nature of the information that would be communicated back to individuals, the media by which results would be communicated (e.g., via the application or with a phone call), and who would deliver the information (e.g., a physician, genetic counselor, or nurse).

5.5 Legal Considerations

Any technology that processes health information—even if the technology does not directly store health information—can face liability issues if the system is breached or compromised. Because dynamic consent solutions are designed for data sharing, they may be at higher risk for allegations of inappropriate access or sharing of individuals' health information (Agarwal et al., 2020). Organizations that offer dynamic consent are encouraged to consult with legal counsel about methods to craft informed consent documentation, data-sharing agreements, breach management strategies, and reduce threats of future litigation (Calvaresi et al., 2019).

6 Future Research

As blockchain-based dynamic consent solutions continue to grow in popularity and sophistication, future research would be valuable to provide directions for these emerging technologies in the following areas:

6.1 More Effective Consent and Communication

Because informed consent is the primary premise behind any dynamic consent solution, it would be valuable to study the most effective methods of describing the application's use, risks, and benefits during the consent process. Considering that much of the dynamic consent information may be provided without interpersonal communication, it is necessary to determine the most understandable dynamic consent wording, including whether it is necessary or appropriate to explain the role of blockchain in a blockchain-based dynamic consent solution. These future consent models should consider the nature of data that may be stored and the likely future sharing and research that could be performed (Angeletti et al., 2018).

Future studies would also benefit from consulting with target populations, including diverse communities, about increasing awareness and engagement with their health information over time. The information gleaned from these studies could inform the nature of technical design and human involvement to ensure that individuals utilize the features intended to empower them with their health information.

6.2 More Effective Design Strategies

Because blockchain-based dynamic consent solutions are in the early stages of development and commercialization, additional research is needed to determine ways of capturing data to demonstrate the benefit of blockchain technology in the architecture. Organizations should conduct rigorous case studies to describe and publish their findings (e.g., Treiblmaier, 2019).

With consideration that blockchain serves as only part of the architecture stack, user interfaces and applications are necessary for users to optimize the underlying blockchain technology. Developers, then, are encouraged to study methods for improving the user experience for perceptions of usefulness, usability, and information quality (Chalil Madathil et al., 2013). These studies could determine the best methods to interact with blockchain features that could create or update smart contracts (e.g., toggle switches, pulldown menus, etc.). These design features are essential for offering choices and facilitating an individual's desire to withdraw (Anabo et al., 2019).

6.3 Better Accountability

Last, blockchain-based dynamic consent concepts require complementary organizational and researcher accountability (Cheung, 2018). Mechanisms for accountability are particularly relevant as more crowdsourced research and citizen scientists would like to access research repositories (Shah et al., 2019). Future studies could determine how to track secondary research to ensure data recipient accountability.

In general, many different types of stakeholders participate in a blockchain-based dynamic consent solution. Future studies would be valuable in determining optimal governance to improve communication and oversight. Research may include learning about the organizational factors necessary to increase trust.

7 Conclusion

Blockchain-based dynamic consent solutions are emerging with the potential to offer individuals more control over their health information while offering efficiencies for data sharing. While dynamic consent capabilities can empower patients, critical questions and considerations remain about enabling trust and engagement with the technology and researchers. The use of blockchain technology could then be viewed as a valuable enablement tool that increases the extent of capabilities and accountability for individuals and organizations. When including blockchain technologies, organizations should consider how to secure initial research participation and increase trust and engagement over time. Ultimately, blockchain-based dynamic consent technologies are believed to offer more visibility into the research enterprise while promoting autonomy and respect for patients and participants.

References

Agarwal, R. R., Kumar, D., Golab, L., & Keshav, S. (2020). Consentio: Managing consent to data access using permissioned blockchains. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON*. IEEE. https://doi.org/10.1109/ICBC48266.2020.9169432

Agbo, C. C., & Mahmoud, Q. H. (2020). Design and implementation of a blockchain-based e-health consent management framework. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Toronto, ON* (pp. 812–817). IEEE. https://doi.org/10.1109/SMC42975.2020.9283203

Albalwy, F., Brass, A., & Davies, A. (2021). A blockchain-based dynamic consent architecture to support clinical genomic data sharing (ConsentChain): Proof-of-çoncept study. *JMIR Medical Informatics, 9*(11), e27816. https://doi.org/10.2196/27816

Albanese, G., Calbimonte, J.-P., Schumacher, M., & Calvaresi, D. (2020). Dynamic consent management for clinical trials via private blockchain technology. *Journal of Ambient Intelligence and Humanized Computing, 11*, 4909–4926. https://doi.org/10.1007/s12652-020-01761-1

Alhajri, M., Salehi Shahraki, A., & Rudolph, C. (2022). Privacy of fitness applications and consent management in blockchain. In *Australasian Computer Science Week 2022, Brisbane, Australia* (pp. 65–73). Association for Computing Machinery. https://doi.org/10.1145/3511616.3513100

Anabo, I. F., Elexpuru-Albizuri, I., & Villardón-Gallego, L. (2019). Revisiting the Belmont Report's ethical principles in internet-mediated research: Perspectives from disciplinary associations in the social sciences. *Ethics and Information Technology, 21*(2), 137–149. https://doi.org/10.1007/s10676-018-9495-z

Angeletti, F., Chatzigiannakis, I., & Vitaletti, A. (2018). Towards an architecture to guarantee both data privacy and utility in the first phases of digital clinical trials. *Sensors (Basel), 18*(12), 4175. https://doi.org/10.3390/s18124175

Appenzeller, A., Hornung, M., Kadow, T., Krempel, E., & Beyerer, J. (2022). Sovereign digital consent through privacy impact quantification and dynamic consent. *Technologies, 10*(1), 35. https://doi.org/10.3390/technologies10010035

Asghar, M. R., & Russello, G. (2012). Flexible and dynamic consent-capturing. In *Open Problems in Network Security, Lucerne, Switzerland* (pp. 119–131). Springer. https://doi.org/10.1007/978-3-642-27585-2_10.

Avdoshin, S., & Pesotskaya, E. (2018). Blockchain revolution in the healthcare industry. In *Proceedings of the Future Technologies Conference (FTC) 2018, Vancouver, BC* (Vol. 1, pp. 626–639). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-02686-8_47

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In I. Awan & M. Younas (Eds.), *IEEE Computer Society Technical Committee on the Internet, 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria* (pp. 25–30). IEEE Computer Society. https://doi.org/10.1109/OBD.2016.11

Ballantyne, A. (2020). How should we think about clinical data ownership? *Journal of Medical Ethics, 46*(5), 289–294. https://doi.org/10.1136/medethics-2018-105340

Barrera, A. Z., Dunn, L. B., Nichols, A., Reardon, S., & Muñoz, R. F. (2016). Getting it "right:" Ensuring informed consent for an online clinical trial. *Journal of Empirical Research on Human Research Ethics, 11*(4), 291–298. https://doi.org/10.1177/1556264616668974

Benchoufi, M., Porcher, R., & Ravaud, P. (2018). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research, 6*. https://doi.org/10.12688/f1000research.10531.5

Bhushan, B., Sinha, P., Sagayam, K. M., & Onesimu, J. A. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers and Electrical Engineering, 90*, 106897. https://doi.org/10.1016/j.compeleceng.2020.106897

Blasimme, A., Moret, C., Hurst, S. A., & Vayena, E. (2017). Informed consent and the disclosure of clinical results to research participants. *The American Journal of Bioethics, 17*(7), 58–60. https://doi.org/10.1080/15265161.2017.1328532

Brall, C., Schröder-Bäck, P., & Maeckelberghe, E. (2019). Ethical aspects of digital health from a justice point of view. *European Journal of Public Health, 29*(Suppl_3), 18–22. https://doi.org/10.1093/eurpub/ckz167

Budin-Ljøsne, I., Teare, H. J. A., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., Collett, C., D'Abramo, F., Felzmann, H., Finlay, T., Javaid, M. K., Jones, E., Katić, V., Simpson, A., & Mascalzoni, D. (2017). Dynamic consent: A potential solution to some of the challenges of modern biomedical research. *BMC Medical Ethics, 18*(1), 4. https://doi.org/10.1186/s12910-016-0162-9

Calvaresi, D., Calbimonte, J.-P., Dubovitskaya, A., Mattioli, V., Piguet, J.-G., & Schumacher, M. (2019). The good, the bad, and the ethical implications of bridging blockchain and multi-agent systems. *Information (Basel), 10*(12), 363. https://doi.org/10.3390/info10120363

Chalil Madathil, K., Koikkara, R., Obeid, J., Greenstein, J. S., Sanderson, I. C., Fryar, K., Moskowitz, J., & Gramopadhye, A. K. (2013). An investigation of the efficacy of electronic consenting interfaces of research permissions management system in a hospital setting. *International Journal of Medical Informatics, 82*(9), 854–863. https://doi.org/10.1016/j.ijmedinf.2013.04.008

Chamber of Digital Commerce. (2018). *"Smart contracts" legal primer*. https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf

Charles, W. M. (2021a). Accelerating life sciences research with blockchain. In S. Namasudra & G. C. Deka (Eds.), *Applications of blockchain in healthcare* (Vol. 83, pp. 221–252). Springer Nature. https://doi.org/10.1007/978-981-15-9547-9_9

Charles, W. M. (2021b). Blockchain for convergence science in mental health. In H. A. Eyre, H. Lavretsky, C. Reynolds 3rd, & M. Berk (Eds.), *Convergence mental health: A transdisciplinary approach to innovation* (pp. 345–359). Oxford University Press. https://doi.org/10.1093/med/9780197506271.001.0001

Charles, W. M. (2021c, July–August). Blockchain innovations in healthcare. *PECB Insights*, (33), 6–11. https://insights.pecb.com/pecb-insights-issue-33-july-august-2021/#page6

Charles, W. M. (2022). Regulatory compliance considerations for blockchain in life sciences research. In W. M. Charles (Ed.), *Blockchain in lifesciences* (pp. 237–266). Springer Nature. https://doi.org/10.1007/978-981-19-2976-2_11

Charles, W. M., & Delgado, B. M. (2022a). Health datasets as assets: Blockchain-based valuation and transaction methods. *Blockchain Healthc Today, 5*, 185. https://doi.org/10.30953/bhty.v5.185

Charles, W. M., & Delgado, B. M. (2022b). Valuing research data: Blockchain-based management methods. In W. M. Charles (Ed.), *Blockchain in life sciences* (pp. 143–173). Springer Nature. https://doi.org/10.1007/978-981-19-2976-2_7

Charles, W. M., & Magtanong, R. (2022). Ethical benefits and drawbacks of digital informed consent. In I. Vasiliu-Feltes & J. Thomason (Eds.), *Applied ethics in a digital world* (pp. 101–123). IGI Global, Information Science Reference. https://doi.org/10.4018/978-1-7998-8467-5.ch008

Charles, W. M., Marler, N., Long, L., & Manion, S. T. (2019). Blockchain compliance by design: Regulatory considerations for blockchain in clinical research. *Frontiers in Blockchain, 2*(18). https://doi.org/10.3389/fbloc.2019.00018

Cheah, P. Y., Jatupornpimol, N., Hanboonkunupakarn, B., Khirikoekkong, N., Jittamala, P., Pukrittayakamee, S., Day, N. P. J., Parker, M., & Bull, S. (2018). Challenges arising when seeking broad consent for health research data sharing: A qualitative study of perspectives in Thailand. *BMC Medical Ethics, 19*(1), 86. https://doi.org/10.1186/s12910-018-0326-x

Chen, C., Lee, P.-I., Pain, K. J., Delgado, D., Cole, C. L., & Campion, T. R. (2020). Replacing paper informed consent with electronic informed consent for research in academic medical centers: A scoping review. *AMIA Jt Summits Transl Sci Proc, 2020*, 80–88. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7233043/

Cheung, A. S. Y. (2018). Moving beyond consent for citizen science in big data health and medical research. *Northwestern Journal of Technology and Intellectual Property, 16*(1), 15–40. https://scholarlycommons.law.northwestern.edu/njtip/vol16/iss1/2/

Chia, V., Hartel, P., Hum, Q., Ma, S., Piliouras, G., Reijsbergen, D., van Staalduinen, M., & Szalachowski, P. (2018). Rethinking blockchain security: Position paper. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS* (pp. 1272–1280). IEEE. https://doi.org/10.1109/Cybermatics_2018.2018.00222.

Custers, B. (2016). Click here to consent forever: Expiry dates for informed consent. *Big Data & Society, 3*(1), 2053951715624935. https://doi.org/10.1177/2053951715624935

De Sutter, E., Meszaros, J., Borry, P., & Huys, I. (2022). Digitizing the informed consent process: A review of the regulatory landscape in the European Union. *Front Med (Lausanne), 9*, 906448. https://doi.org/10.3389/fmed.2022.906448

Department of Health and Human Services. (2011, August 19). *Guidance on exculpatory language in informed consent*. Retrieved July 13, 2019, from https://www.hhs.gov/ohrp/regulations-and-policy/requests-for-comments/guidance-exculpatory-language/index.html

Despotou, G., Evans, J., Nash, W., Eavis, A., Robbins, T., & Arvanitis, T. N. (2020). Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the dovetail digital consent application: A cross sectional exploratory study. *Digit Health, 6*, 2055207620924949. https://doi.org/10.1177/2055207620924949

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018). Smart contracts vulnerabilities: A call for blockchain software engineering? In R. Tonelli, S. Ducasse, G. Fenu, & A. Bracciali (Eds.), *2018 International Workshop on blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy* (pp. 19–25). IEEE Computer Society. https://doi.org/10.1109/IWBOSE.2018.8327567

Dulhanty, A. (2021). Present value of future health data: Ethics of data collection and use. *Bulletin of the World Health Organization, 99*(2), 162–163. https://doi.org/10.2471/BLT.19.237248

Electronic Signatures in Global and National Commerce Act. (2000). *Pub L, 106–229, 114 Stat. 464 (June 30, 2000)*. https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

European Medicines Agency. (2022). *Clinical Trial Regulation* (536/2014). https://www.ema.europa.eu/en/human-regulatory/research-development/clinical-trials/clinical-trials-regulation.

General Data Protection Regulation, European Parliament and the Council of the European Union. (2016). https://gdpr-info.eu/ and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Gibbons, S. M. C., Kaye, J., Smart, A., Heeney, C., & Parker, M. (2007). Governing genetic databases: Challenges facing research regulation and practice. *Journal of Law and Society, 34*(2), 163–189. https://www.jstor.org/stable/20109740

Hartley, A. M. (2022). *Trust as a differentiator: Protecting human data In your products and services*. Retrieved August 22, 2022, from https://burstiq.com/trust-as-a-differentiator-protecting-human-data-in-your-products-and-services-burstiq/

Huh, K. Y., Jeong, S.-u., Moon, S. J., Kim, M.-J., Yang, W., Jeong, M., Song, I., Kwak, Y.-G., Lee, S., & Kim, M.-G. (2022). METORY: Development of a demand-driven blockchain-based dynamic consent platform tailored for clinical trials. Front Med (Lausanne), 9(3389), 837197. https://doi.org/10.3389/fmed.2022.837197.

International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use. (2016). *ICH Harmonized guideline integrated addendum to ICH E6(R1): Guideline for good clinical practice E6(R2)*. https://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E6/E6_R2__Step_4_2016_1109.pdf

Jacobs, B. (2021). *Integrating consent management techniques into blockchain-based medical data sharing* Delft University of Technology]. Delft. http://resolver.tudelft.nl/uuid:b40c42e6-4369-46cf-a49a-4d50123ff505

Jaiman, V., & Urovi, V. (2020). A consent model for blockchain-based health data sharing platforms. *IEEE Access, 8*, 143734–143745. https://doi.org/10.1109/ACCESS.2020.3014565

Jung, H. H., & Pfister, F. M. J. (2020). Blockchain-enabled clinical study consent management. *Technology Innovation and Management Review, 10*(2), 14–24. https://doi.org/10.22215/timreview/1325

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). A systematic review of blockchain for consent management. *Healthcare (Basel), 9*(2), 137. https://doi.org/10.3390/healthcare9020137

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H. J. A., & Melham, K. (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics, 23*(2), 141–146. https://doi.org/10.1038/ejhg.2014.71

Kim, T. M., Lee, S.-J., Chang, D.-J., Koo, J., Kim, T., Yoon, K.-H., & Choi, I.-Y. (2021). DynamiChain: Development of medical blockchain ecosystem based on dynamic consent system. *Appl Sci (Basel), 11*(4), 1612. https://doi.org/10.3390/app11041612

Lacity, M. C., & Khan, S. (2019). Exploring preliminary challenges and emerging best practices in the use of enterprise blockchain applications. In T. X. Bui (Ed.), *52nd Hawaii International Conference on System Sciences, Grand Wailea, HI* (pp. 4665–4674). University of Hawaii. http://hdl.handle.net/10125/59904

Learney, R. (2019). Blockchain in clinical trials. In D. Metcalf, J. Bass, M. Hooper, A. Cahana, & V. Dhillon (Eds.), *Blockchain in healthcare: Innovations that empower patients, connect professionals and improve care* (pp. 87–108). CRC Press, Taylor & Francis Group. https://www.routledge.com/Blockchain-in-Healthcare-Innovations-that-Empower-Patients-Connect-Professionals/Dhillon-Bass-Hooper-Metcalf-Cahana/p/book/9780367031084

Leon-Sanz, P. (2019). Key points for an ethical evaluation of healthcare big data. *PRO, 7*(8), 493. https://doi.org/10.3390/pr7080493

Mamo, N., Martin, G. M., Desira, M., Ellul, B., & Ebejer, J.-P. (2019). Dwarna: A blockchain solution for dynamic consent in biobanking. *European Journal of Human Genetics, 28*, 609. https://doi.org/10.1038/s41431-019-0560-9

Merlec, M. M., Lee, Y. K., Hong, S.-P., & In, H. P. (2021). A smart contract-based dynamic consent management system for personal data usage under GDPR. *Sensors, 21*(23), 7994. https://doi.org/10.3390/s21237994

Muravyeva, E., Janssen, J., Specht, M., & Custers, B. (2020). Exploring solutions to the privacy paradox in the context of e-assessment: Informed consent revisited. *Ethics and Information Technology, 22*, 223–238. https://doi.org/10.1007/s10676-020-09531-5

National Conference of Commissioners on Uniform State Laws. (1999). *Uniform Electronic Transaction Act*. http://euro.ecom.cmu.edu/program/law/08-732/Transactions/ueta.pdf

Office for Civil Rights. (2008, December 15). *How do HIPAA authorizations apply to an electronic health information exchange environment?* Retrieved June 29, 2019, from https://www.hhs.gov/hipaa/for-professionals/faq/554/how-do-hipaa-authorizations-apply-to-electronic-health-information/index.html

Office for Human Research Protections. (2016, December). *Informed consent FAQs*. Retrieved June 14, 2019, from https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/informed-consent/index.html

Office for Human Research Protections. (2017, July 26). *Recommendations for broad consent guidance*. Retrieved November 11, 2022, from https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-c-august-2-2017/index.html

Ploug, T., & Holm, S. (2016). Meta consent – A flexible solution to the problem of secondary use of health data. *Bioethics, 30*(9), 721–732. https://doi.org/10.1111/bioe.12286

Porsdam Mann, S., Savulescu, J., Ravaud, P., & Benchoufi, M. (2021). Blockchain, consent and prosent for medical research. *Journal of Medical Ethics, 47*, 244–250. https://doi.org/10.1136/medethics-2019-105963

Rahimzadeh, V. N. (2021). Pros and cons of prosent as an alternative to traditional consent in medical research. *Journal of Medical Ethics, 47*, 251–252. https://doi.org/10.1136/medethics-2020-106443

Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C., Papanikolaou, A., & Kritsas, A. (2019). ADvoCATE: A consent management platform for personal data processing in the IoT using blockchain technology. In J.-L. Lanet & C. Toma (Eds.), *Innovative security solutions for information technology and communications, Bucharest, Romania* (Vol. 11359, pp. 300–313). Springer International Publishing. https://doi.org/10.1007/978-3-030-12942-2_23

Robinson, J. O., Slashinski, M. J., Wang, T., Hilsenbeck, S. G., & McGuire, A. L. (2013). Participants' recall and understanding of genomic research and large-scale data sharing. *Journal of Empirical Research on Human Research Ethics, 8*(4), 42–52. https://doi.org/10.1525/jer.2013.8.4.42

Rothstein, M. A., Harrell, H. L., Saulnier, K. M., Dove, E. S., Fan, C. T., Hung, T.-H., Nnamuchi, O., Obadia, A., Siegal, G., & Knoppers, B. M. (2018). Broad consent for future research: International perspectives. *IRB: Ethics & Human Research, 40*(6), 7–12. https://doi.org/10.1002/eahr.406002

Rupasinghe, T., Burstein, F., & Rudolph, C. (2019). Blockchain based dynamic patient consent. In *40th International Conference on Information Systems, Munich, Germany* (Vol. 14).

Association for Information Systems. https://aisel.aisnet.org/icis2019/blockchain_fintech/blockchain_fintech/14/

Schuler Scott, A., Goldsmith, M., & Teare, H. J. A. (2019). Wider research applications of dynamic consent. In E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, & S. Krenn (Eds.), *Privacy and identity management fairness, accountability, and transparency in the age of big data, Vienna, Austria* (pp. 114–120). Springer International Publishing. https://doi.org/10.1007/978-3-030-16744-8_8

Shah, M., Li, C., Sheng, M., Zhang, Y., & Xing, C. (2019). *CrowdMed: A blockchain-based approach to consent management for health data sharing. Smart Health, Shenzhen, China* (Vol. 11924, pp. 345–356). Springer International Publishing. https://doi.org/10.1007/978-3-030-34482-5_31

Shrestha, A. K., Vassileva, J., & Deters, R. (2020). A blockchain platform for user data sharing ensuring user control and incentives. *Frontiers in Blockchain, 3*(48), 497985. https://doi.org/10.3389/fbloc.2020.497985

Spanò, R., Massaro, M., & Iacuzzi, S. (2021). Blockchain for value creation in the healthcare sector. *Technovation, (Forthcoming)*, 102440. https://doi.org/10.1016/j.technovation.2021.102440

Taylor, M. J., & Whitton, T. (2020). Public interest, health research and data protection law: Establishing a legitimate trade-off between individual control and research access to health data. *Laws, 9*(1), 6. https://doi.org/10.3390/laws9010006

Tith, D., Lee, J.-S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthc Inform Res, 26*(4), 265–273. https://doi.org/10.4258/hir.2020.26.4.265

Treiblmaier, H. (2019). Toward more rigorous blockchain research: Recommendations for writing blockchain case studies. *Frontiers in Blockchain, 2*(3). https://doi.org/10.3389/fbloc.2019.00003

U.S. Food and Drug Administration. (2017, June). *Guidance for industry: Use of electronic records and electronic signatures in clinical investigations under 21 CFR Part 11 - questions and answers (draft)*. Retrieved October 11, 2020, from https://www.fda.gov/media/105557/download

Velmovitsky, P. E., Miranda, P. A. D. S. E. S., Vaillancourt, H., Donovska, T., Teague, J., & Morita, P. P. (2020). A blockchain-based consent platform for active assisted living: Modeling study and conceptual framework. *Journal of Medical Internet Research, 22*(12), e20832. https://doi.org/10.2196/20832

Verde, F., Stanzione, A., Romeo, V., Cuocolo, R., Maurea, S., & Brunetti, A. (2019). Could blockchain technology empower patients, improve education, and boost research in radiology departments? An open question for future applications. *Journal of Digital Imaging, 32*, 1112–1115. https://doi.org/10.1007/s10278-019-00246-8

Wee, R. (2013). Ethics: Dynamic consent in the digital age of biology. *Journal of Primary Health Care, 5*(3), 259–261. https://doi.org/10.1071/HC13259

WMA Declaration of Helsinki - ethical principles for medical research involving human subjects: Adopted by the 64th WMA General Assembly, Fortaleza, Brazil. (2013, March 21). World Medical Association. Retrieved January 19, 2020, from https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

WMA Declaration of Taipei on ethical considerations regarding health databases and biobanks: Revised by the 67th WMA General Assembly, Taipei, Taiwan, October 2016. (2016, March 21). World Medical Association. Retrieved January 19, 2020, from https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/

Dr. Wendy Charles has been involved in clinical trials from every perspective for 30 years, with a strong background in operations and regulatory compliance. She currently serves as a Chief Ethics and Compliance Officer for Equideum Health, a healthcare information technology company specializing in next-gen person-centered healthcare and research networks. She is also an adjunct faculty member in the University of Colorado Denver and the University of Denver. Dr. Charles augments her blockchain healthcare experience by serving on the EU Blockchain Observatory and Forum Expert Panel, HIMSS Blockchain Task Force, Government Blockchain Association healthcare group, and IEEE Blockchain working groups. She is also involved as an assistant editor and reviewer for academic journals. Dr. Charles obtained her Ph.D. in Clinical Science with a specialty in Health Information Technology from the University of Colorado, Anschutz Medical Campus. She is certified as an IRB Professional, Clinical Research Professional, and Blockchain Professional.

"Pay for Value": Blockchain for Drug Pricing in Canada

Precilia Kong, Chang Lu, and Citlali Cruz

Abstract

Value-based pricing (VBP) in healthcare refers to payment based on the quality of care delivered or healthcare outcomes and has not been broadly implemented. Although in its infancy, Distributed Ledger Technologies or DLTs (e.g., Blockchain) have emerged as a potential solution for Canada's chronic data obstruction problem through gathering cost information and patient experience metrics that are currently dispersed. In this chapter, we identify potential barriers for the implementation of VBPs in Canada by conducting a literature review, and examine how leveraging DLTs can address those barriers through a combination of qualitative (Grounded Theory; GT) and quantitative analyses. Results show that among three identified categories of barriers for VBPs implementation, infrastructural and economic ones are most critical. Based on the empirical activities and findings, we give recommendations on how smart contract can be deployed to facilitate VBPs implementation and which blockchain platform should be considered for building smart contracts.

P. Kong
Faculty of Medicine, University of British Columbia, Vancouver, BC, Canada

C. Lu (✉)
Blockchain@UBC, University of British Columbia, Vancouver, BC, Canada
e-mail: chang.lu@ubc.ca

C. Cruz
Independent Consultant on Policy, Technology and Immigration, Montréal, QC, Canada

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_4

1 Introduction

All over the world, pharmaceutical drugs represent a large amount of healthcare expenditure. In 2020, the average expenditure on drugs is xxx per person. Partly because of the exceedingly high drug price, pharmaceutical companies are negatively perceived by the public despite their contributions to drug development. To lower the price of medications, academics, industry leaders, and policy makers have attempted various methods, but drug cost remains high.

In recent years, blockchain has emerged as a promising technology to transform healthcare. Although different use cases of blockchain have been proposed for healthcare, for example, drug supply chain, personal health wallet, and clinical data exchange (reference), the use of blockchain for drug pricing has not been explored.

Aiming to fill this gap, in this chapter, we investigate how blockchain technology may facilitate the shift toward value-based pricing, enabling payers to pay for the value they receive from medications and thereafter decreasing the expenditure on drugs. We ground our investigation in Canada not only because drug pricing varies greatly among countries and focusing on one country would allow targeted investigation, but also because Canada has attempted value-based drug pricing such that we are provided with more information to analyze.

To explore the benefits of blockchain for drug pricing in Canada, we first conduct a systematic literature review on the Canadian drug pricing landscape, revealing the structure and evolution of the system, previous and current pricing policies, and the barriers for the shift toward value-based pricing. We then explain the nature of blockchain, demonstrate how it may help overcome some of the barriers, and provide adoption recommendations. We contribute to the literature not only by providing the first systematic analysis of the technical and ecosystem parameters of adopting blockchain for drug pricing, but also by serving as an example of how to analyze the feasibility of blockchain for particular domains in healthcare.

2 Drug Pricing in Canada: A Literature Review

To thoroughly understand drug pricing in Canada, we conducted a literature review on the practice of drug pricing and the evolution of the practice, and found that although Canada attempted to shift toward value-based pricing but economic, infrastructural, and legal barriers have hindered progress. In this section, we explain the literature search and selection strategy and then describe our findings.

2.1 Methods

We adopted the systematic literature review method. First, three health science databases (MEDLINE, EMBASE, and Web of Science Core Collection) were accessed through the library of an international university and used for this search.

Table 1 Database search terms

Database	Search terms
MEDLINE, EMBASE (https://www.ovid.com/)	TOPIC: ((value based adj2 (agreement* or contract* or reimburs* or drug or payment or pricing)) AND (drug* or prescription* or medication*) AND (outcomes based adj2 (agreement* or contract* or reimburs* or drug or payment or pricing)) AND (drug* or prescription* or medication*)
Web of Science Core Collection (https://webofknowledge.com)	TOPIC: (value based agreement* or value based contract* or value based pricing) AND (reimbursement or pricing) AND (drug or medication or prescription) AND Canada*) AND ((outcomes based agreement* or value based contract* or value based pricing) AND (reimbursement or pricing) AND (drug or medication or prescription) AND Canada*)
Google Scholar (https://scholar.google.com/)	(value based or outcomes based) AND (drug reimbursement or drug pricing) AND Canada

* . . .

Google Scholar was utilized to augment the search and capture any remaining articles related to the research question. The first 10 pages of Google Scholar were reviewed and relevant literature that was not previously included were recorded. An informal process of including papers based on targeted searches and reviewing references of exact topic papers was carried out. Reimbursement policies, economic and drug pricing reports as well as grey literature carried out within Canada were also reviewed.

Publications were identified by applying the MESH indexes to generate related search terms to envelope a broader scope of peer-reviewed literature and grey literature. The main keywords were "exploded" in order to include the more specific terms underneath that heading, if applicable (Table 1). The goal of this search was to draw out the largest number of papers in relation to the research questions while maintaining methodological coherence.

All types of documents in English were included; however, restrictions were applied to the date of publication. An initial screening of the results by title and abstract scan was carried out, followed by a review of the full text of the preselected articles. Previous works were excluded if one of the following exclusion criteria was met:

1. The introduction of the pan-Canadian Pricing Alliance in August of 2010 galvanized changes within the reimbursement and drug pricing (Husereau et al., 2014). Thus, in order to ensure the inclusion of the most relevant and up-to-date articles, papers that were published prior to 2010 were excluded
2. The country of interest was not Canada or did not include Canada as one of the countries explored

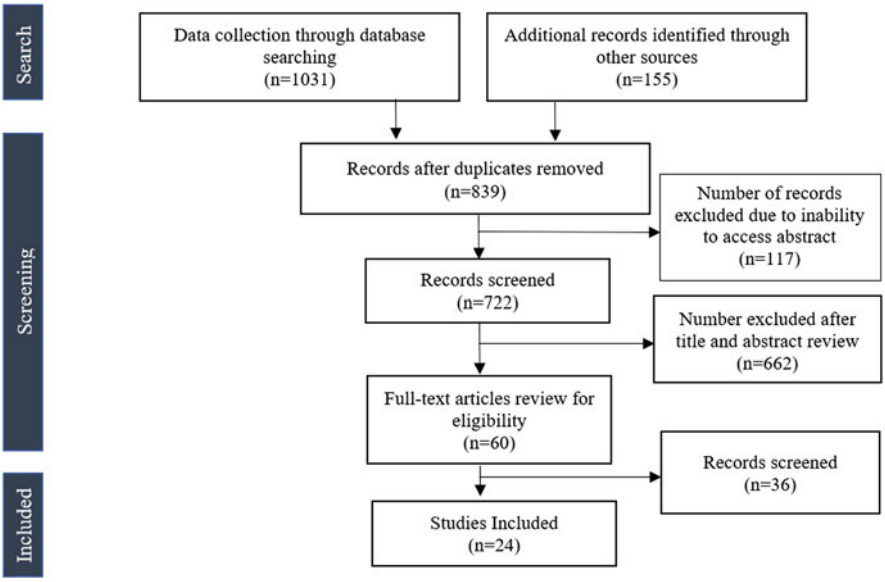


Fig. 1 Flowchart of database search strategy

3. The topic examined pricing and reimbursement models for a specific drug or drugs (i.e., too specific) or

   The topic was unrelated to research question described above.

In total, 1186 records were collected and exported to an excel spreadsheet in order to conduct further assessments. Among the 1186 articles collected from the initial search, all duplicates ($n = 347$) were removed. Out of the remaining eligible articles ($n = 722$), a thorough title and abstract scan, as well as a subsequent full-text review for eligibility was conducted in order to exclude ($n = 662$) irrelevant papers. After reviewing the remaining 60 articles, only 24 papers were included in the final analysis (Fig. 1). Descriptive statistics of the papers included after the full-text review are summarized in Table 2.

2.2 The Current Practice of Drug Pricing in Canada

In Canada, there is no provision for mandatory universal coverage for drugs (Husereau et al., 2014; Paris & Belloni, 2014; Nanson & Chuck, 2013; Anis, 2000). Rather, the governments of each province and territory make coverage decisions and establish formularies—a list of pharmaceutical drugs covered by a prescription drug plan they manage in their jurisdiction (Anis, 2000). Across health plans, the extent of coverage for pharmaceuticals varies, in terms of both the eligible population (e.g., elderly or individuals with disabilities) and the types of drugs

Table 2 Descriptive statistics ($n = 24$)

Criteria	*n* (%)
Publication year	
2010	1 (4.2)
2011	1 (4.2)
2012	1 (4.2)
2013	4 (16.6)
2014	3 (12.5)
2015	3 (12.5)
2016	1 (4.2)
2017	2 (8.2)
2018	1 (4.2)
2019	6 (25.0)
2020	1 (4.2)
Location of focus	
Canada only	17 (70.8)
Included Canada[a]	7 (29.2)
Publication type	
Meeting abstracts	1 (4.2)
Discussion paper	1 (4.2)
Review	5 (20.8)
Institutional report	3 (12.5)
Research article	14 (58.3)

[a]Canada was included as one of the countries of focus (e.g., a study focused on the international perspective but included Canada as one of the countries)

included on the formulary list (Husereau et al., 2014). In Canada, all inpatient medications are covered (Brougham et al., 2017). There are also federally funded and delivered drug plans for first nations (non-insured health benefits), veterans, penitentiary inmates, armed services personnel, and the federal police. Due to continually increasing drug prices and the growing pressures to fund new technologies, expenses on pharmaceuticals have become one of the highest healthcare expenditures in Canada (Rizzardo et al., 2019). Provincial and territorial governments are spending in excess of 40% of their budgets on drug coverage and around two-thirds of Canadians rely on privately funded drug insurance programs or pay out of pocket for pharmaceutical expenses (Husereau et al., 2014; Rizzardo et al., 2019).

The pathway for drug pricing in Canada is complex (Fig. 2). For a manufacturer to market a pharmaceutical in Canada, Health Canada reviews the efficacy, safety, and quality of data to determine marketing approval (Brougham et al., 2017). If deemed marketable by Health Canada, manufacturers will receive either a Notice of Compliance (NOC) or NOC with conditions (NOC/c). The Patented Medicine Prices Review Board (PMPRB) is the federal body that provides pricing approval for brand pharmaceuticals in Canada (Prieto-Pinto et al., 2020; Brougham et al., 2017; Paris & Belloni, 2014).

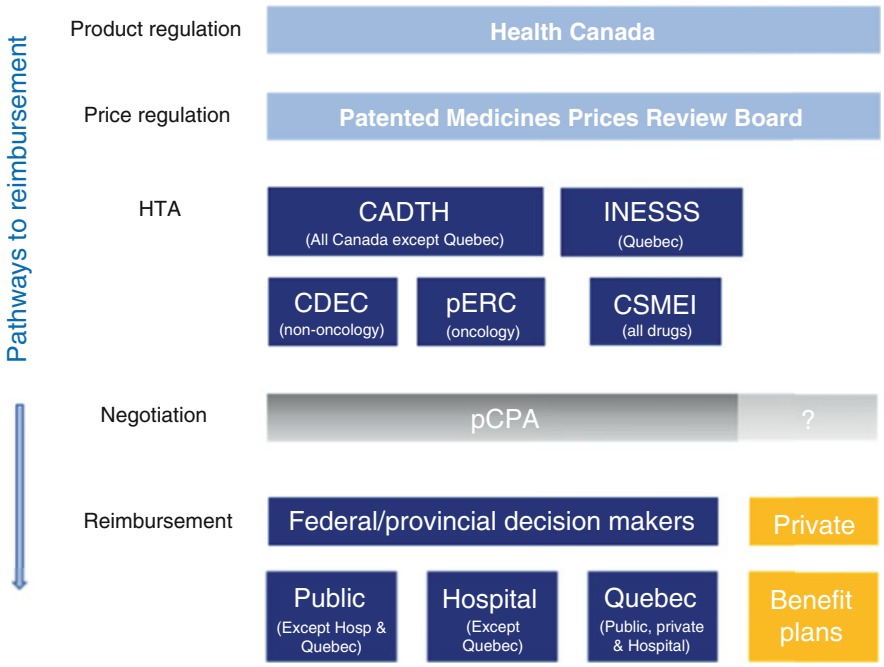


Fig. 2 Pathway to reimbursement as of August 2017 (Brougham et al., 2017)

The PMPRB acts in a regulatory capacity, to protect Canadians and ensure that prices charged for patented medicines are not excessive (Paris & Belloni, 2014). Under the current guidelines, PMPRB prices of new patented medicines are assigned a ceiling price based on degree of therapeutic benefit relative to existing drugs. Once this maximum allowable price is set, it enters the market (Prieto-Pinto et al., 2020; Paris & Belloni, 2014). It should be noted that the board is not responsible for regulating off-patent drugs, such as generics (Brougham et al., 2017).

The Canadian Agency for Drugs and Technology in Health (CADTH) operates two pan-Canadian drug review processes: the CADTH pan-Canadian Oncology Drug Review (pCODR), which deals specifically with cancer drugs, and the CADTH Common Drug Review (CDR), which deals with non-oncology drugs (CADTH, 2020). The goal of the pCODR was to bring consistency and clarity to the assessment of cancer drugs (Milliken et al., 2015). These intergovernmental collaborative bodies exist to critically assess the evidence for effectiveness and safety, and to define, capture, and reward value creation, with the goal of making decisions that are fiscally responsible without sacrificing patient health (Prieto-Pinto et al., 2020; Milliken et al., 2015).On behalf of all public payers (with exception of hospitals and Quebec), CADTH reviews comparative and cost effectiveness data and provides listing recommendations. Although the recommendations are intended to improve the consistency of listing decisions, participating drug programs have varying capacities to implement the recommendation and often require

contextualizing recommendations to the unique reimbursement environments (e.g., resource constraints or local priorities) (Husereau et al., 2014; Paris & Belloni, 2014).

While Health Canada, PMPRB, and CADTH (INESSS—the equivalent of CADTH in Quebec) provide policy framework and regulatory oversight, the pan-Canadian Pricing Alliance (pCPA) manages the negotiation of drug price. The pCPA was introduced in August 2010 and has transformed the industry-payer landscape (Husereau et al., 2014), serving as a governing body for joint provincial, territorial, and federal value negotiations for brand and generic drugs (Husereau et al., 2014; Prieto-Pinto et al., 2020). By leveraging on the combined negotiating power of drug plans across the provinces and territories, the pCPA aims to enhance patient access to clinically relevant and cost-effective drug treatment options, as well as improve the consistency of drug listing decisions (Husereau et al., 2014; Prieto-Pinto et al., 2020; Paris & Belloni, 2014; Milliken et al., 2015; Vogler et al., 2019).

In 2015, the alliance underwent a formal name change, with pCPA now standing for pan-Canadian Pharmaceutical Alliance (pCPA, 2020). During this time, the alliance also developed a mandate and objectives, developed a governance structure, and had an office created to provide support to the member jurisdictions. During this year, Quebec also joined the alliance and in 2016, the federal drug plans joined including the Non-Insured Health Benefits (NIHB), Correctional Services of Canada (CSC), and Veterans Affairs Canada (VAC).

Negotiations under the pCPA generally occur in the following stages as illustrated by Fig. 2 (pCPA, 2020).

1. *Pre-pCPA*: To prevent a duplication of efforts, the pCPA has partnered with CADTH and INESSS to receive any materials from manufacturers which are shared with the HTA (Health technology assessment) bodies at pre-submission meetings.
2. *Phase 1: Initiation*: If a drug is new, the pCPA process begins once a recommendation is published by CADTH and/or INESSS. The office of pCPA (pCPAO) issues an Acknowledgement Letter to the manufacturer. If the drug already exists and is publicly funded in one or more jurisdiction, the pCPA process may be initiated by the pCPA upon review of funded drug products. New products that are a new version or an enhancement of one of the manufacturers existing drugs (i.e., line extension) are subject to jurisdictional review, processes, and approvals.
3. *Phase 2 or Consideration*: In this phase, the pCPA decides whether negotiations should take place. The factors taken into consideration include affordability, therapeutic landscape, HTA recommendation, and current coverage of alternative drugs. Once a decision is made, the following may occur: (1) an Engagement Letter is sent to the manufacturer to express the pCPA's interest in engaging in negotiations, (2) a Hold Letter is sent to the manufacturer that the pCPA will not engage in negotiations for a certain period of time to await further information to negotiate individually, or (3) collectively decide not to negotiate a price at all and send a Close Letter to the manufacturer.

4. *Phase 3: Negotiation*: The drug will enter the negotiation phase once the manufacturer receives an Engagement Letter. The jurisdictions leading the negotiations will reach out to the manufacturer to outline next steps and may request a proposal. This proposal will help to facilitate negotiations (usually meetings in person or through teleconference) and the sharing of information to participating jurisdictions. During this process, negotiators from both the pCPA and manufacturers are expected to be knowledgeable of the landscape while the information shared (e.g., pricing information or budget impact estimates) will be held in confidence. To ensure efficiency, effectiveness, and integrity of the process, negotiations are managed in a way that is free from political, media, and patient influences. Although participation from each jurisdiction is sought out, only a subset of jurisdictions in agreement may proceed to an LOI, depending on each jurisdiction's particular circumstances and value assessments.
5. *Phase 4*: Completion: Two outcomes can result from the negotiation step. If a mutual understanding of terms is reached, a letter of intent (LOI) is executed; however, if agreement is not reached, the pCPAO issues a Close Letter that the negotiation is closed.
6. *Post-pCPA*: After the LOI is signed, manufacturers negotiate product listing agreements (PLA) with each participating jurisdiction based on the terms in the LOI. Jurisdictions which choose to opt out of the LOI will not be able to independently negotiate with the manufacturer for the drug. However, at a later date, should any jurisdiction not listed in the LOI wish to fund the drug at a later date, the pCPAO will issue a notification to the manufacturer to amend the LOI. This new jurisdiction may then enter its own PLA with the manufacturer.

3 Attempts for Value-Based Pricing and the Barriers for Adoption

In May 2013, the Institute of Health Economics held a National Roundtable on product listing in light of the move to the pCPA for pharmaceutical reimbursement (Nanson & Chuck, 2013). It emphasized the need for accountability, transparency, and confidentiality of the negotiations and agreements that are brought forward to the pCPA. There are considerable opportunities to increase the use of economic evaluation and value-based pricing in a formal pCPA process. Applying value-based pricing both across provinces and drug classes could add significant value to pricing decisions for patients and the public by increasing access and efficacy (Paris & Belloni, 2014; Nanson & Chuck, 2013).

Although not a new concept, literature surrounding value-based pricing within the drug coverage landscape in Canada is scarce and only has emerged in the last decade or so (Nanson & Chuck, 2013). After reviewing the literature, three categories of barriers—economic, infrastructural, and legal considerations—emerged repeatedly in discussions around adopting value-based pricing during PLA negations. These themes are summarized in Table 3.

Table 3 Infrastructural, legal, and economic barriers associated with the implementation of VBPs

Barrier		Description	Consequences	Recommendations
Economic	Inefficiencies within the processes of valuing drugs	• Lack of involvement of key stakeholders (e.g., HCPs or community members) during discussions of value (Nanson & Chuck, 2013) • Payers' concepts of value influenced by a combination of health benefits and political constraints (Garrison & Towse, 2017; Nanson & Chuck, 2013)	Concepts of value that are not reflective of *societal ideals* and result in complex and lengthy negotiations (Husereau et al., 2014; Garrison & Towse, 2017; Prieto-Pinto et al., 2020; CADTH, 2020; Milliken et al., 2015; Nanson & Chuck, 2013; Dranitsaris et al., 2012)	Move toward more *transparency* and *stakeholder involvement* within the pricing and reimbursement process to increase efficiencies (Drummond, 2013)
	Incentivizing research and development (R&D)	• Balancing reductions in price without affecting investment into R&D (Garrison & Towse, 2017; Prieto-Pinto et al. 2020; Nanson & Chuck, 2013) • Industry considers value-based pricing to include the concept of valuing innovation itself, not just the impact of that innovation (Nanson & Chuck, 2013)	VBP policy consists of negotiating prices of new pharmaceutical products based on the value that the new medicine offers to society. Lower prices may result in manufacturers losing incentives for innovating new drugs/ technologies and R&D (e.g., orphan drugs) (Garrison & Towse, 2017; Prieto-Pinto et al. 2020; Nanson & Chuck, 2013)	Rewarding manufacturers for the net health gain and cost-offsets in the responder target population. (Garrison & Towse, 2017)
Infrastructural	The fragmentation of the delivery of healthcare	• As Canada does not have a universal drug plan, the	• There is a lack of coordination across Canada's federal,	• Opportunities to reduce duplication and leverage shared resources

(continued)

Table 3 (continued)

Barrier		Description	Consequences	Recommendations
		governments of each province make decisions regarding the public funding of drugs (Prieto-Pinto et al., 2020) • Differences in policy institutions and structures, and demographic difference for drug programs in provinces and territories (Husereau et al., 2014; Prieto-Pinto et al., 2020) • Variable participation by provinces and territories in proceeding to an LOI during the pCPA negotiation process (Husereau et al., 2014; Paris & Belloni, 2014; Nanson & Chuck, 2013).	provincial, territorial, and private insurance programs leading to inefficiencies in pricing negotiations and promotes "post-code" prescribing (Husereau et al., 2014; Prieto-Pinto et al., 2020; Nanson & Chuck, 2013). • Complex negotiations, as a result of provinces and territories opting for individual negotiations in situations where the jurisdictions do not see coordinated negotiation as feasible, may result in delay or failure to reach a negotiation conclusion (Husereau et al., 2014; Paris & Belloni, 2014; Nanson & Chuck, 2013).	through the coordination among public insurance programs (Husereau et al., 2014) • Increased *spending power* results in the potential for faster listing decisions and incentivizes better discounts (especially for smaller provinces/territories) (Husereau et al., 2014; Prieto-Pinto et al., 2020; CADTH, 2020; Nanson & Chuck, 2013)
	Lack of resources and capacity for adoption	• Putting innovative agreements in place is a costly business and requires the ability to monitor approach and collect subsequent data. (Brougham	Value-based pricing cannot be materialized through ongoing implementation	Ongoing development of frameworks to assess when to use VBA approaches (e.g., what type of drug) (Husereau et al., 2014; Prieto-Pinto et al., 2020; Nanson & Chuck, 2013)

(continued)

Table 3 (continued)

Barrier		Description	Consequences	Recommendations
		et al., 2017) • Lack of resources (i.e., budget and human resources) needed to adopt value-based pricing in a cost-effective manner (Husereau et al., 2014; Prieto-Pinto et al., 2020; Nanson & Chuck, 2013)		
Political/legal	No legal structure for the pCPA	• No legal structure for pCPA that gives rise to specific obligations for manufacturers and provinces/territories (e.g., no legally binding time frames for negotiations). (Husereau et al., 2014) • There is a lack of governing rules to establish how each stakeholder should and should not be interacting with each other, and their obligations. (Husereau et al., 2014)	Lack of consistency in how to capture value and integrate value into PLA negotiations	Accountability needs to be carefully considered for all parties when fostering agreements (Husereau et al., 2014)
	Confidentiality of negotiations	Industry has a business model that is set up to provide confidential deals to provinces. (Husereau et al., 2014)	• There is a lack of publicly accessible information regarding negotiations, which hinders the measurement of value	Inclusion of nondisclosure agreements in VBAs and permitting exemptions may allow information to be shared among all

(continued)

Table 3 (continued)

Barrier		Description	Consequences	Recommendations
			• Because of international reference pricing, disclosure of information that can impact the price manufacturers' offer in other countries. (Husereau et al., 2014)	constituents. (Husereau et al., 2014)

3.1 Infrastructural Barriers

The development of the pCPA has placed a question mark over the role that value-based pricing (VBP) could play in the Canadian context (Nanson & Chuck, 2013; Anis, 2000). The pCPA brought together provincial and territorial governments to collaborate on a coordinated approach to price negotiation and address the incoherence between federal regulation of drugs and provincial requirement for pricing drugs. Currently, provinces can maintain separate PLAs, however, this leads to the duplication of negotiation and bureaucracy by both government and manufacturers.

Effective PLAs and VBP require an appropriate infrastructure for collective evidence on value, as well as an infrastructure for developing and managing agreements, and sharing evidence across the participating stakeholders (Nanson & Chuck, 2013). Also, it is important that each stakeholder in the process understands their role and has the capacity and skills to take on the role (Husereau et al., 2014; Prieto-Pinto et al., 2020; Nanson & Chuck, 2013). However, there are major issues around the capacity to deliver value-based PLAs on both sides of the agreement (Brougham et al., 2017). Public payers have only small human resources to engage in PLAs, which are easily stretched considering the number of new drugs that can come to market each year (Prieto-Pinto et al., 2020). Industry face problems around the capacity to engage in evidence development. While pharmaceutical firms may have the manpower to go into complex negotiations, the ability to access evidence on the uptake is underdeveloped (Husereau et al., 2014; Prieto-Pinto et al., 2020; Nanson & Chuck, 2013). Whatever the mechanism, the literature supports the need to prevent "postal-code prescribing" and to understand the capacities of those involved within the existing infrastructure (Nanson & Chuck, 2013).

3.2 Economic Issues

Internationally, value-based pricing is typically implemented through two main approaches—assessments based on overall economic impact and the use of clinical benefit or disease specific value scales (Prieto-Pinto et al., 2020).

Within the landscape of pharmaceutical pricing and reimbursement, there is a synergy felt by industry, policymakers, and payers in wanting to improve access to new drugs for patients through pooling resources and creating a more nuanced understanding of what value means (Husereau et al., 2014; Prieto-Pinto et al., 2020; CADTH, 2020; Nanson & Chuck, 2013). Value has predominantly been measured as improvements in overall health (e.g., QALYs), but there are wider elements of value that could be applied (pCPA 2020s), such as cost effectiveness.

As part of a democratic system, decision makers are expected to inform value-related decision with an evidence-based understanding of societal values that reflect the public's (i.e., taxpayers) priorities and interests. Issues arise as value can mean different things to different people (Garrison & Towse, 2017; Brougham et al., 2017; CADTH, 2020; Nanson & Chuck, 2013; Dranitsaris et al., 2012). For example, payers' concepts of value are tied to the net health benefit of the implementation of a therapeutic, whereas industry's value takes into account the value of innovation itself or the R&D costs (Garrison & Towse, 2017; Nanson & Chuck, 2013). Interestingly, healthcare providers themselves are often not explicitly involved in the deliberations as to how new drugs are valued.

Another quandary around the value of drugs is that value of cost-savings achieved through new therapeutics and drugs is often not linked back to the budgets of those payers pricing the drugs ("harvesting" savings) (Brougham et al., 2017). This is an issue for payers who wish to see improvements in health and the health system, but whose actions are assessed only against the cost of the drug and not its full range of budget impacts.

3.3 Political and Legal Issues

In addition to the challenges identified above, there exist several political and legal issues that must be taken into consideration when thinking about the adoption of VBP.

The current business model in Canada is set up to ensure the confidentiality of information during price negotiations and is a central concern for manufacturers. While this is acknowledged by all stakeholders, there is a desire for increased transparency around the pCPA processes and outcomes of agreements to allow for payers to be accountable to the public (Husereau et al., 2014).

Currently, there is no legal structure for the pCPA that specifies obligations for the provinces and territories, nor for the manufacturers (Husereau et al., 2014). There is a lack of governing rules to establish how each stakeholder should and should not be interacting with each other, and their obligations. For example, provinces or territories can sign a LOI on completion of the pCPA; however, they are under no

legal obligation to list the product on their formulary within a particular time frame. This creates uneasiness for manufacturers who negotiate with the government but are not supported by actual commitment. Based on the literature, accountability, transparency, and confidentiality need to be carefully considered when improving drug pricing agreements through the pCPA, the lack of which not only hinders the negotiation of PLAs in general but also makes it hard to embed value into the negotiations since the conception and measurement of value is opaque to begin with.

4 Using Blockchain to Facilitate the Adoption of Value-Based Pricing

In the previous section, we revealed the current practice of drug pricing in Canada, the attempts to adopt value-based pricing, and the economic, infrastructure, and policy/legal barriers. In the following section, we analyze how blockchain can be used to facilitate the adoption of value-based pricing.

4.1 Blockchain: What Is It?

Blockchain, a distributed ledger technology, is a consensus of replicated, shared, and synchronized digital information that are not stored by any central entity (Klein, 2018; Nogueira, 2017). More specifically, blockchain consists of shared, immutable (i.e., unchanging) records of peer-to-peer transactions built from linked "blocks" and stored within a digital ledger (i.e., database of transactions) (Yong et al., 2013). Information being decentralized is one of the key elements of the blockchain system: this means that records are stored, exchanged, and viewed across all network participants ("peer-to-peer"). However, records can only be added to the database, never removed, with each new record cryptographically linked to all previous records in time. New records can only be added based on synchronous agreement or "distributed consensus" of those maintaining the database. Trust and transparency are reinforced within the system by requiring the verification of new information by the network before it is stored within the system. By cryptographically linking the records it is impossible for one party to manipulate previous records without breaking the overall consistency of the database.

4.2 Blockchain in Healthcare

It has been proposed that blockchain has the potential to transform healthcare and solve current inefficiencies by promoting access to shared data among trusted parties, increasing the interoperability of health data, and gathering cost, quality, and patient-specific metrics that are currently dispersed in data silos (Klein, 2018). When storing healthcare data in a blockchain, cryptography is used for encrypting the contents of a message or transaction, so that only intended users can open and

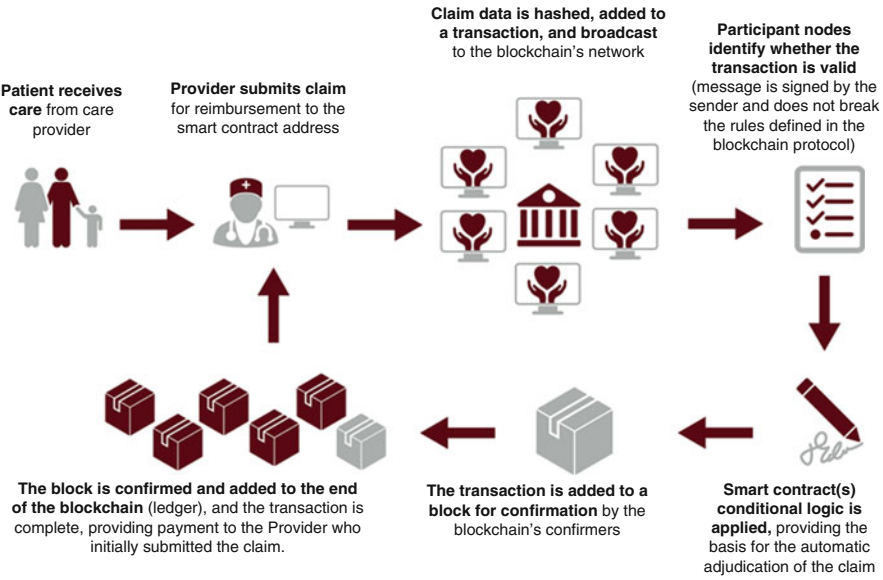


Fig. 3 One example of data flow architecture for processing blockchain-enabled health care claims (Klein, 2018)

read its contents. The encryption process works via "Public Key Cryptography" or asymmetric cryptography, an encryption system that uses pairs of keys. First, a "public key" may be disseminated widely to everyone and a "private key" that is known only to its holder. Either key may be used to encrypt a message, but the other key must decrypt the message. Practically speaking, there are two use cases involving public and private keys. A patient can encode her health data with a public key and be sure that only the holder of the private key can correspond with public key. It is guaranteed that the holder of the private key is the party that encrypted the data. Such a process is equivalent to "signing" a message because it is analogous to someone putting her unique signature on a document.

Better data sharing between healthcare providers results in timely and accurate diagnoses, more effective treatments, and the overall increased ability of healthcare systems to deliver cost-effective care (Nogueira, 2017). Klein (2018) provides one example of using blockchain technology for clinical pathway programs that require total data recall for contract reconciliation (Fig. 3).

4.3 How Can Blockchain Facilitate the Adoption of Value-Based Pricing?

4.3.1 Research Procedure

To understand how blockchain can facilitate the adoption of value-based pricing in Canada, we performed content analysis on academic and industry articles as well as

Table 4 Database search terms

Database	Search terms	# of results
Google Scholar (https://google.ca/)	((value based agreement* or value based contract* or value based pricing* or outcomes based agreement) AND (blockchain or distributed ledger tech*) AND (reimbursement or pricing) AND (drug or medication or prescription) AND Canada)	9

the scripts of conversations with industry experts. We collected the articles by web-searching the terms displayed in Table 4, and recruited conversation participants within the researchers' Linked network. Web research results were restricted to those in the English language and published between January 1st, 2015 and December 31st, 2020, while the conversations with experts are semi-structured to ensure consistency. Note that since the discussion about blockchain for value-based pricing is at early stage, we were only able to collect a limited number of articles and conversations for content analysis (nine articles and three conversations).

Despite that the material for our content analysis is limited, we performed systematic analysis of the material by following Vaismoradi et al.'s (2016) study and the Gioia et al.'s method (Gioia et al. 2013). This includes the development of a codebook, as well as first-order and second-order concepts which then emerge into "aggregate dimensions."

Table 5 shows the codebook. In order to ensure validity of the codebook, we went through randomly chosen first-order and second-order concepts with a research assistant. If there were areas of discordance or confusion, we worked together to ensure that the language appropriately encompassed the idea.

In order to make sense of the qualitative data, we organized the concepts in a way that exposed common higher-level themes to answer the aforementioned research questions. These aggregate dimensions as well as the relationship between concepts are displayed in Fig. 4.

Next, to better understand how the adoption barriers for value-based pricing can be alleviated by blockchain, we worked to understand how the second order codes and aggregate dimensions in Fig. 4 interacted with one another. Figure 5 summarizes this process and helps to expose which barriers would be prime areas of focus when considering the use of DLTs within the pharmaceutical landscape, and especially to ease the adoption of VBAs.

4.3.2 Findings

Our analysis suggests that there is a shared understanding among researchers and industry experts that the adoption of blockchain can enable stakeholders in drug-pricing to clearly communicate and understand their roles, since smart contracts can be used to functionally manage or automate stakeholders' activities, while the distributed ledger improves data security and transparency for internal and external

Table 5 Codebook

Name	Files	Ref.
Benefits of data sharing is more efficient (administratively) and more economic (cost-effective)	6	11
Blockchain enables data sharing between multiple parties	3	5
Blockchain ideally suited to address trust issues	7	8
Blockchain will transform and improve healthcare	8	17
Blockchain-supported wearables and patient-centric care can help with patient-reported outcomes and value-based care	5	7
Blockchain and DLTs have clear audit trail for data which prevents forgery, hacking, falsification of data, and promotes trust within the system	4	6
Blockchain has elements of privacy that ensure data protection	3	3
Blockchain moves healthcare toward a decentralized model	3	3
Blockchain can enable electronic informed consents (eConsent) which offers huge improvements to participant on-boarding, a guarantee of validity, and documentation of the consent process in future clinical trials	2	3
Decentralization ensures fair pricing of drugs and reduces the risk of monopolies on drugs. This makes drugs more affordable and accessible for patients	4	7
Incentivizing a global blockchain ecosystem and participation from a variety of different stakeholders	2	4
Current healthcare infrastructure is poorly suited for value-based care, but Blockchain and DLTs can address these issues	2	3
Blockchain will enable interoperability which will help to move toward precision medicine era	1	2
One can leverage smart contract features in blockchain technology which have many benefits especially in value-based agreements	7	16
Self-sovereign ownership allows patients to make decisions about who has access to their information and encourages more patient involvement in decision-making and their own healthcare	4	12
Electronic Health Records (EHRs) can be built upon blockchain platforms and provides the opportunity for the monetization over one's own patient data	4	8
Blockchain can make it easier to synthesize data from IoT devices for chronic disease management, remote monitoring, or patient-provider communication, enabling fee-for-value systems	3	3
The role of artificial intelligence and blockchain technology	3	3
Working toward defining value for patients (patient-reported outcomes)	7	15
Ethereum is one of the best platforms for a blockchain solution in healthcare because of its capacity for smart contracts and other complicated computing capacities	3	4
Having access to functioning blockchain platforms can improve data sharing and IP issues in research and development	3	5
Blockchain can be used in supply chain tracking and tracing, especially for pharmaceutical companies	3	5
Adoption will take at least a decade for the infrastructure to be in place	1	1

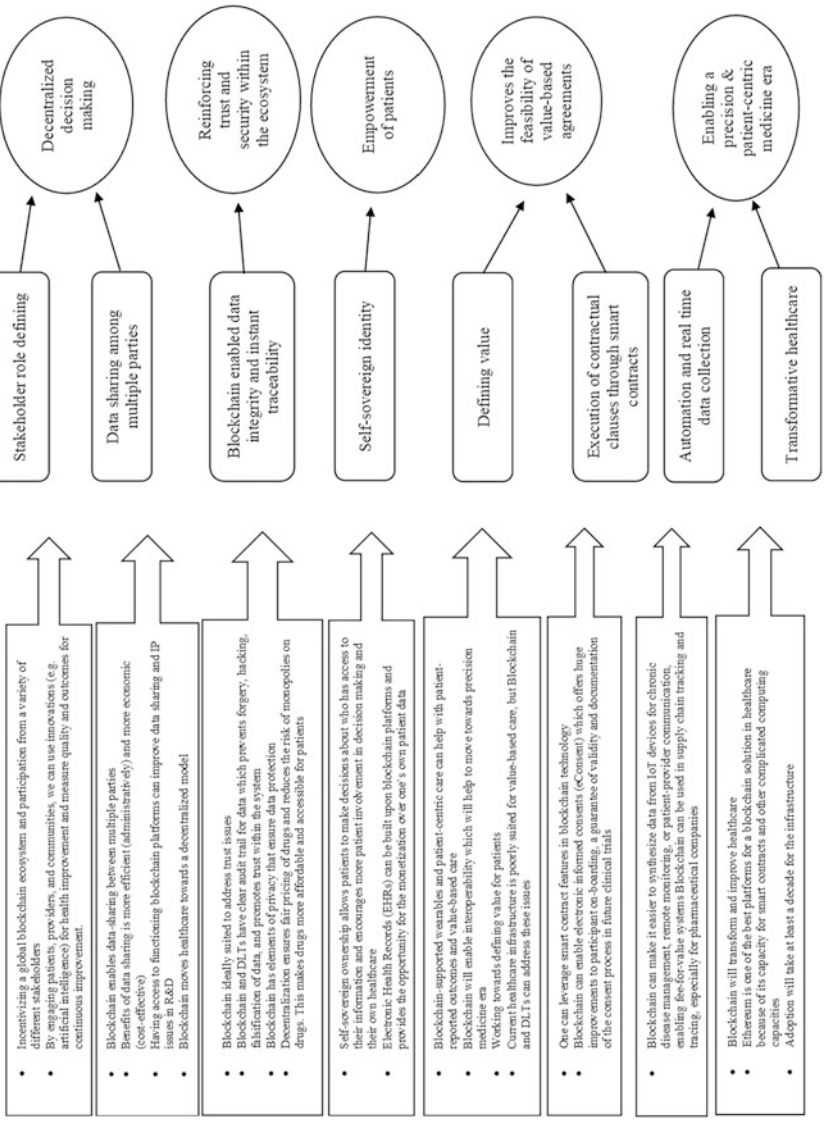


Fig. 4 Data structure

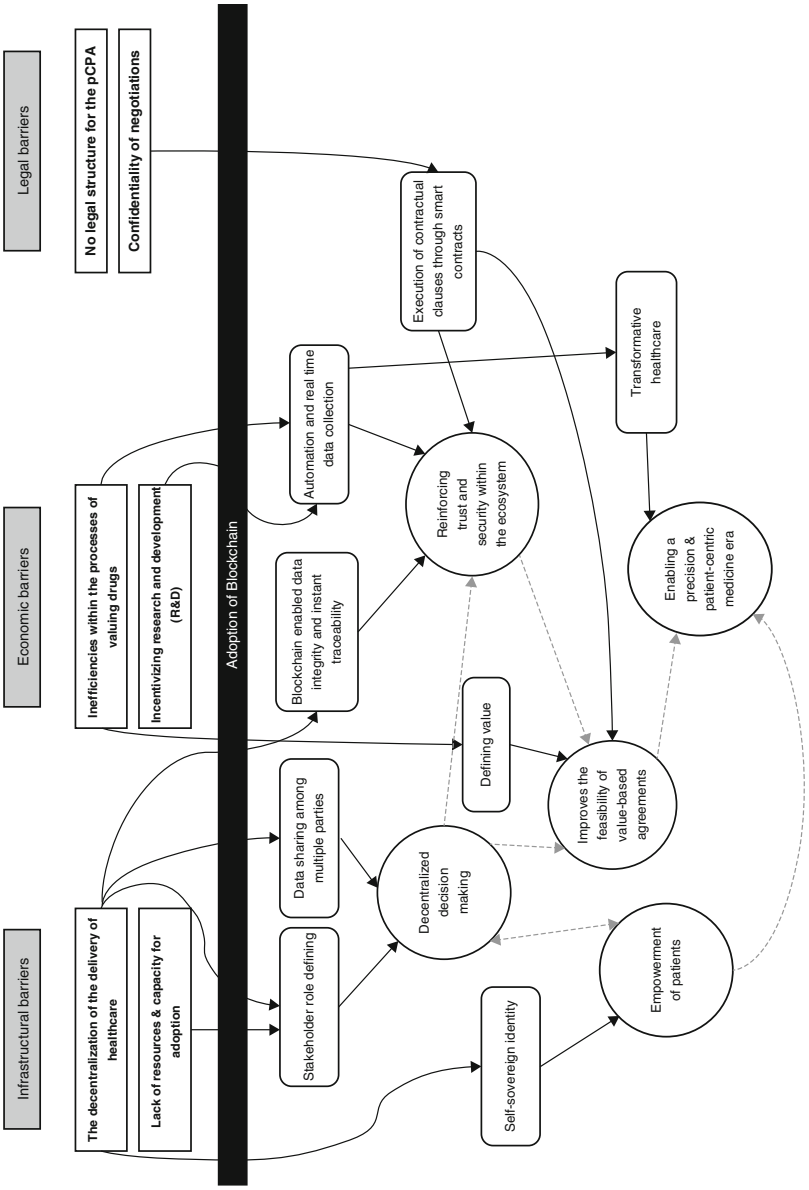


Fig. 5 Impact of the adoption of Blockchain on infrastructural, economic, and legal barriers

business units as well as collaborators, with fine-grained verification and authorization of participants.

Blockchain integration into existing health systems, especially with the drug reimbursement landscape, would enable health-care interoperability across health-care institutions with a means to verify the entire history of a health-care record back to its creation with mathematical certainty of the provenance and integrity. Interoperability not only means having the capability to exchange confidential information but also being able to use the exchanged information. To give an example: blockchain technology may have a special benefit in the claims process. To determine the cost shares, the health plan must first validate services received from the provider against the agreement they share, as well as any applicable regulatory requirements for that interaction.

The distributed ledger design and validated transaction block features make blockchain fit for clinical pathway programs that require total data recall for contract reconciliation. All patient-level data from multiple sources can be recorded in a secure and privacy protected environment, validated to ensure it links to the correct unique individual, and then indelibly stamped in the ledger with a unique cryptographic signature, thus leaving an auditable history (which reinforces trust within the system). Data would be almost real time and usable for continuous quality improvement—a key feature in furthering the ultimate goals of VBP (value-based pricing) in creating a learning health system. The traditional data vendors of today would need to adapt to a world where the costs of data acquisition will drop dramatically, as there would be no more "tollgate" B2B agreement to pass through for the purposes of data exchange. No longer would VBP be burdened with the crushing overhead costs and paucity of data in today's fragmented, data-hoarding environment. Future contracts could be done with easily agreed upon rules regarding accessing patient data, which could be permissioned among the contract participants.

The blockchain-based VBP ecosystem would be a virtuous circle that begins with the adoption of electronic health records (EHRs) and ends with the measurement of quality parameters and outcomes. In between, we make Personal health information (PHI) interoperable and secure, build the capability to aggregate and normalize data, and then deploy big-data strategies to create actionable information that translates into clinical or performance insights. Artificial intelligence can manage data streams in determining correct courses of action on an individual basis, augmented by digital-clinical products in the patient engagement space. Ultimately, by engaging patients, providers, and communities, we can use innovations for health improvement and measure quality and outcomes for continuous improvement.

Once unblocked, primary data sets that are needed for effective VBAs, including clinical data, claims data, and sociodemographic data, would be able to integrate to provide a holistic and longitudinal view of the impact of pharmacotherapy on a patient and patients in a population. A better understanding of specific therapies on specific patients would be possible, helping not only VBCs, but also lightening the burdens of post-marketing surveillance. As blockchain is an excellent tool for provenance and security, only the appropriate data will be accessed, at low to no

risk, and this data will be permissioned by the patient (as opposed to permission-less blockchain networks, such as Bitcoin).

Besides, blockchain can facilitate the negotiation of the actors involved in value-based pricing. In Canada, drug prices are negotiated between provinces and manufacturers, in which each province does not have access to prices agreed between the manufacturer and other provinces or to the terms of the agreements. In this case, blockchain could serve as a platform for all negotiators to interact with each other and provide one single version of the truth. For example, it can serve for the sharing of agreements or status of negotiations between provinces; manufacturer and provinces can also share information regarding the volume of sales; assessment institutions can also share information with provinces regarding the functioning of a certain drug. Overall, easing the sharing of information could contribute to the decreasing of information asymmetry in negotiation processes between parties.

In addition, blockchain could enhance the transparency of the negotiation process as negotiating parties can record and broadcast negotiation stages and outcomes via the distributed ledger, including interim price, rebates, or discounts. Furthermore, the privacy-preserving property of blockchain can enable the inclusion of treatment outcomes that could ease the evaluation of specific medications' effectiveness while keeping the information confidential.

5 Recommendation: Consortium Blockchain Architecture on Hyperledger Fabric

The analysis above suggests that blockchain can facilitate the adoption of value-based pricing (VBP). In this section, we offer design insights into blockchain-based VBP, aiming to precipitate deeper discussions about adopting blockchain for VBP. Note that our design is targeted at the Canadian system, as different countries may have different policy and architecture requirements.

We propose that permissioned blockchains built on Hyperledger Fabric may be feasible for VBP, for which consortiums can be introduced for governance. A consortium consists of a few organizations where procedures are set up and controlled by the preliminary assigned users. We recommend using the Hyperledger Fabric protocol, due to the fact that it was made for enterprises and enables permissioned architecture, and is therefore more applicable for drug-pricing compared to completely permission-less protocols. Additionally, it comes with a wide range of consensus algorithms, pluggable options, multiple ledger formats, and many more. As one can imagine, users can customize this platform to a great extent. However, if smart contracts are prioritized features of a blockchain-based payment system, then one needs to consider using Hyperledger Besu, which allows the interoperability between smart contracts created via Ethereum and the enterprise blockchain consortium based on Hyperledger.

Figure 6 highlights the use of smart contracts in blockchain-based drug-pricing systems in Canada where multiple stakeholders (i.e., patients, manufacturers, and the pCPA) are interacting. A drug enters the "Negotiation Phase" once the Manufacturer

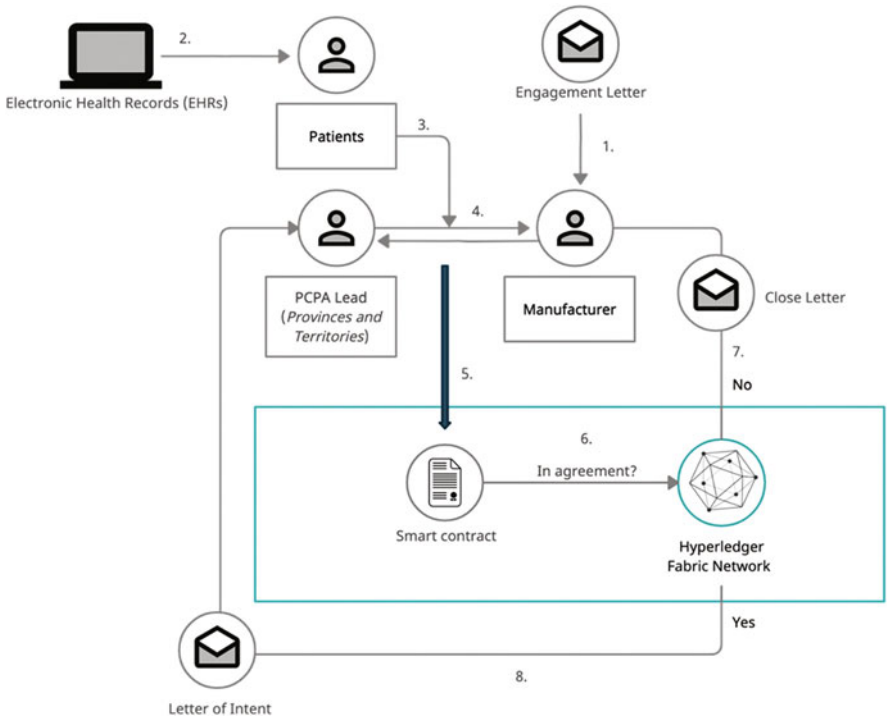


Fig. 6 Smart contract for drug pricing negotiation scenario

receives an Engagement Letter [1]. Value-based purchasing agreements are created when drug manufacturers and purchasers negotiate costs of a drug based on patient health outcomes or financial incentives. Blockchain technology also enables to develop patient-reported outcome measures (PROMs) or ensure electronic health records (EHRs), which include indicators of disease state, dietary changes, lifestyle issues, pain levels, or disease management experiences [2]. Drug developers, as well as healthcare providers, should integrate this type of patient-provided data into their data stream, care routines, and decision-making processes [3]. In these agreements, health insurers negotiate with private pharmaceutical companies to receive rebates, discounts, or other incentives based on a drug's effectiveness in treating a disease [4].

No longer would one have to wait months for a rebate, instead value can flow freely across multiple parties in real time. Terms of a contract can be programmed into a smart contract, applying business logic and updating the contract when actions are taken as well as when outcomes are met [5]. Defining appropriate rules in the smart contract for healthcare will be crucial and must include the consent of all the relevant parties. In the healthcare blockchain, the patient and other stakeholders in the network should set up their details and sign the agreement for accepting the terms in order to develop the requirements in the smart contract. All of this would be

adjudicated by a neutral and shared protocol; ultimately helping us scale VBPs [6]. The pCPA process is considered complete once the negotiation has resulted in mutually agreed upon terms and a fully executed LOI [7], or, if mutually agreed upon terms are not reached, a Close Letter will be sent to the Manufacturer, indicating that the negotiation is closed [8]. Depending on whether these conditions are met, the contract will automatically execute and the transaction containing information about the data arrives to the address of the smart contract, then the distributed virtual machine of the blockchain executes the programming code process.

6 Conclusions

The misalignment between infrastructure and goals makes it difficult to realize value-based pricing in Canada. However, blockchain opens up a wealth of possibilities to transform the healthcare system, especially within the drug pricing and reimbursement landscape. Currently, there are a few start-ups such as Lyfegen© (Lyfevalue) and Healthverity© (Curisium Inc.) developing blockchain-based platforms to allow payers, providers, and life science companies to efficiently and securely engage in innovative, patient-centric, value-based contracts. While these efforts may lead to creative destruction in the current hierarchy of data ownership, the net benefits of adoption of blockchain are clear. We call for stronger commitment to patient care excellence and the use of new tools and technologies such as blockchain to bring us to more information-driven and value-harnessed health care.

References

About pCPA. pan-Canadian Pharmaceutical Alliance website. Accessed December 6, 2020., from https://www.pcpacanada.ca/about

Anis, A. H. (2000). Pharmaceutical policies in Canada: Another example of federal-provincial discord. *CMAJ, 162*(4), 523–526. https://www.cmaj.ca/content/162/4/523.short

Brougham, M., O'Neil, W., & Samaha, D. (2017). *Canada reimbursement profile*. Regulatory Affairs Professionals Society. https://www.raps.org/regulatory-focus%E2%84%A2/news-articles/2017/10/canada-reimbursement-profile

CDR Guidelines, Procedures, and Templates. CADTH website. Accessed December 2, 2020., from https://cadth.ca/about-cadth/what-we-do/products-services/cdr/common-drug-review-submissions/guidelines-procedures-templates

Dranitsaris, G., Truter, I., Lubbe, M. S., Cottrell, W., Spirovski, B., & Edwards, J. (2012). The application of pharmacoeconomic modelling to estimate a value-based price for new cancer drugs. *Journal of Evaluation in Clinical Practice, 18*(2), 343–351. https://doi.org/10.1111/j.1365-2753.2010.01565.x

Drummond, M. (2013). Twenty years of using economic evaluations for drug reimbursement decisions: What has been achieved? *Journal of Health Politics, Policy and Law, 38*(6), 1081–1102. https://doi.org/10.1215/03616878-2373148

Garrison, L. P., Jr., & Towse, A. (2017). Value-based pricing and reimbursement in personalised healthcare: Introduction to the basic health economics. *Journal of Personalized Medicine, 7*(3), 10. https://doi.org/10.3390/jpm7030010

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Husereau, D., Dempster, W., Blanchard, A., & Chambers, J. (2014). Evolution of drug reimbursement in Canada: The pan-Canadian pharmaceutical alliance for new drugs. *Value in Health, 17*(8), 888–894. https://doi.org/10.1016/j.jval.2014.08.2673

Klein, I. (2018). Blockchain, data obstruction, and the promise of information sharing for a value-based health care world. *Journal of Clinical Pathways, 4*(7), 27–30. https://doi.org/10.25270/jcp.2018.09.00035

Milliken, D., Venkatesh, J., Yu, R., Su, Z., Thompson, M., & Eurich, D. (2015). Comparison of drug coverage in Canada before and after the establishment of the pan-Canadian pharmaceutical Alliance. *BMJ Open, 5*(9), e008100. https://doi.org/10.1136/bmjopen-2015-008100

Nanson, E., & Chuck, A. (2013). *Provincial industry-payer agreements in an era of national pricing strategies: National roundtable*. 2013 June. https://www.ihe.ca/advanced-search/provincial-industry-payer-agreements-in-an-era-of-national-pricing-strategies-national-roundtable-final-report

Nogueira, E. (2017) Blockchain in value-based healthcare. LinkedIn Blogs. 2017 Dec 4. https://www.linkedin.com/pulse/blockchain-value-based-healthcare-ernesto-nogueira/

Paris V., & Belloni, A. (2014). *Value in pharmaceutical pricing—Country profile: Canada*. Organisation for Economic Co-operation and Development (OECD). https://www.oecd.org/canada/Value-in-Pharmaceutical-Pricing-Canada.pdf

Prieto-Pinto, L., Garzón-Orjuela, N., Lasalvia, P., Castañeda-Cardona, C., & Rosselli, D. (2020). International experience in therapeutic value and value-based pricing: A rapid review of the literature. *Value in Health Regional Issues, 23*, 37–48. https://doi.org/10.1016/j.vhri.2019.11.008

Rizzardo, S., Bansback, N., Dragojlovic, N., Douglas, C., Li, K. H., Mitton, C., & Lynd, L. D. (2019). Evaluating Canadians' values for drug coverage decision making. *Value in Health, 22*(3), 362–369. https://doi.org/10.1016/j.jval.2018.08.008

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. https://doi.org/10.5430/jnep.v6n5p100

Vogler, S., Zimmermann, N., Haasis, M. A., Babar, Z. U. D., Busse, R., Balbino, J. E., & Wirtz, V. J. (2019). Conference 2019: Medicines access challenge–The value of pricing and reimbursement policies. *Journal of Pharmaceutical Policy and Practice, 12*(3), 34. https://doi.org/10.1186/s40545-019-0194-x

Yong, J. H., Beca, J., & Hoch, J. S. (2013). The evaluation and use of economic evidence to inform cancer drug reimbursement decisions in Canada. *PharmacoEconomics, 31*(3), 229–236. https://doi.org/10.1007/s40273-012-0022-5

Precilia Kong (she/her) is a first-year medical student at the University of British Columbia (UBC) with a diverse background in neuroscience, public health, and healthcare delivery. She holds a Bachelor of Science in Integrated Sciences and a Master of Public Health from UBC. Precilia's research interests include healthcare systems, global health, and knowledge translation, and she has conducted research on neurodevelopmental disorders, early childhood education, and mental health literacy. Her master's degree focused on cultural humility, access to medical services, and knowledge translation, which led her to spend nine months in Japan researching gaps in mental health care access during the COVID-19 pandemic. Before starting medical school, she worked with Vancouver Coastal Health on the COVID-19 response and promoted more patient-centered research for youth and their caregivers/families at Foundry BC's Knowledge Translation team. Precilia is interested in exploring innovative approaches to improve health outcomes, and she sees the potential for Distributed Ledger Technologies (DLTs), such as blockchain, to revolutionize healthcare delivery by gathering cost information and patient experience metrics that are currently dispersed.

Chang Lu is currently the cluster manager at Blockchain@UBC, the University of British Columbia, where he completed his postdoc research on blockchain adoption in healthcare. His theoretical research focuses on technology adoption, organization and institutional change, and the interplay between culture and power. He has published several articles in leading management journals and taught senior undergraduate and MBA students Organizational Strategy and Organizational Behavior. He serves as the supervisor of master and MBA students for their research projects and is currently creating education materials for executives about blockchain in healthcare. He earned his Ph.D. in Strategic Management and Organization, School of Business, from the University of Alberta. Prior to his academic career, he worked as an HR professional in China and Europe.

Citlali Cruz holds a Master in Public Policy and Global Affairs from the University of British Columbia. With a background in law, Citlali became a regulated immigration consultant as her background in policy and innovation proved to be valuable in this field and she was able to provide clients with a unique perspective on the ever-changing laws and regulations. Citlali remains passionate about policy and innovation and continues to explore the potential of technology to improve the lives of immigrants in Canada.

A Blockchain-Centric Data Sharing Framework for Building Trust in Healthcare Insurance

Wenping Zhang, Ruiyun Xu, J. Leon Zhao, and Qiqi Jiang

Abstract

Data sharing is very important in the healthcare insurance industry, given that a premium claim often needs data from multi-parties, such as patients, hospitals, banks, and insurance companies. Generally, data sharing only occurs when sufficient trust exists among the multiple parties involved with the claim. However, since fierce competition and lack of trust may exist among some of these parties, willingness of data sharing may be severely restricted in healthcare insurance. Furthermore, healthcare data are private and sensitive. Risk of privacy disclosure is also a major problem we must consider for managing shared data in healthcare insurance. As blockchain has been proposed in recent years as a potential solution to enable multi-party trust, we develop in this article a blockchain-centric data sharing framework to resolve the trust problem in the context of healthcare insurance. Specifically, we construct a trusted data sharing platform built on blockchain where each party uploads their encrypted data to the blockchain while the immutability of blockchain prevents any data tampering and

W. Zhang
Renmin University of China, Beijing, China
e-mail: wpzhang@ruc.edu.cn

R. Xu
Shenzhen Research Institute of Big Data, Chinese University of Hong Kong (Shenzhen), Shenzhen, China
e-mail: ruiyunxu@cuhk.edu.cn

J. L. Zhao (✉)
Chinese University of Hong Kong (Shenzhen), Shenzhen, China
e-mail: leonzhao@cuhk.edu.cn

Q. Jiang
Copenhagen Business School, Frederiksberg, Denmark
e-mail: qj.digi@cbs.dk

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_5

the traceability of blockchain helps identify attacks to the data immediately after they happen. Moreover, we also develop zero-knowledge-proof mechanisms to ensure that data verification can be made without any disclosure of data specifics.

1 Introduction

Collaboration is one of the most significant characters in modern economy, especially dealing with complex issues. Efficient collaboration calls for effective data sharing. Much previous research has revealed that trust is the prerequisite for data sharing (e.g., Karvounarakis et al., 2013; Pinjani & Palvia, 2013; Verma & Sinha, 2016). However, trust building is time-and-energy consuming and trust is easy to be breached (Kumar, 1996), which has become one of the most serious shackles for the development and continuation of collaboration. The trusted third party plays a significant role in traditional solutions of data sharing. Nevertheless, considering the enormous value embedded in the data and the superpower the trusted third party has, it would be a serious temptation for the third party. Many real cases in recent years have shown that the so-called trusted third party is not always trustworthy, which makes the situation of data sharing more difficult. The emerging new information technology, such as blockchain, brings opportunity for this critical problem. In a blockchain-based data sharing process, a data owner only needs to upload the encrypted data to the chain. The asymmetric encryption technology guarantees that only users with permission can access the data (Zhu, 2016). Given that there is no actual "keeper" of the data, the limitation of trust no longer exists. Thus, blockchain technology is extremely suitable for data exchange and sharing among multiple parties.

An insurance, especially long-term care insurance (LTCI), is a typical business scenario that needs collaboration and data sharing among multiple parties (e.g., insured, insurer, hospitals, and nursing homes), and the parties are related to each other because of insurance activities (e.g., application, claim, and reimbursement). For example, in the scenario of LTCI, the government assigns an insurance company as the leading insurer and all others as agent insurers in a city. Both the leading insurer and agent insurers can sell LTCI to their customers. However, the leading insurer also plays the role of supervisor, who has the right to monitor the activities related to LTCI in agent insurers. The leading insurer acts as "both player and judge at the same time" in this scenario making the relationships among these parties very complex. These complex relationships bring the biggest and primary challenges to effectively authenticate files submitted by different parties given that there is no chance for trust construction in this scenario. Furthermore, insurers are competing for consumers. Such competition makes them less likely to trust each other and their submitted files. Considering the huge benefits embedded in the transactions, high data tampering risk exists in the file transmission process. In current practice, parties mainly rely on the use of application programming interface (hereinafter API) to synchronize data from different and isolated systems with disparate data schema.

However, this synchronization process is neither effective nor trustworthy. The APIs should be predefined before the design of a system, and any changes or malfunctions will lead to a crash of the whole system. The keeper of APIs has the superpower of the system. Furthermore, it is vulnerable to attacks (e.g., a man-in-the-middle attack). Thus, the API-based system could increase the transaction cost in the data sharing among parties.

Research on information technology resistance has pointed out the fact that technology can contribute to practice only when it is used (Davis et al., 1989). Unfortunately, resistance for new technology is ubiquitous, especially in a traditional field like insurance (Lapointe & Rivard, 2005). Blockchain is considered a disruptive technology (Frizzo-Barker et al., 2020), which presents many differences compared with other widely used technologies. The uncertainty of this disruptive technology will bring high system switching risk during adoption and increase transition cost. Additionally, data verification is a common need in data exchange and sharing. In the traditional API-based approach, the verification is very straightforward where data are stored and exchanged in plaintext format. However, since plaintext can be accessed by anyone, data security (e.g., privacy protection in healthcare) has become a serious challenge. Encryption can guarantee the security of the data but adds verification cost simultaneously. In many existing blockchain applications, encrypted data need to be deciphered before verification. However, the data will lose its protection when deciphered and cause high privacy leakage risk. This dilemma is a critical issue we must address when we develop healthcare data sharing systems. Although encryption mechanism could enhance the data security (e.g., attacks), it does not always work when conducting verification since data need to be decrypted before verification in traditional approaches. In other words, this encryption–decryption verification approach significantly increases data verification cost without really decreasing privacy leakage risk.

To resolve the abovementioned challenges and dilemmas, we propose a blockchain-based system, for real practice of LTCI in collaboration with a Fortune 500 insurance company in China. Our proposed blockchain-based system used blockchain technology to solve the trust dilemma so as to reduce the transaction cost among multi-parities in LTCI data sharing. The data are stored in the Merkle tree format on the blockchain for the convenience of auditing. Smart contracts are also designed to guarantee the data are shared accurately and timely. To reduce the resistance to the new technology, we designed a middle layer in the format of software development kit (SDK) to connect LTCI's participants' existing systems and the new blockchain-based system. The middle layer will guarantee that few changes and specific training are needed to deploy the new system. In this way, the transition cost can be significantly reduced. In addition, we also implement a novel protocol with zero-knowledge proof in our blockchain-based system. It could verify encrypted information without any sensitive information disclosure to reduce the verification cost. As such, the proposed blockchain-based system has significant contributions in terms of (1) a blockchain-based framework to reduce the transaction cost, (2) a middle layer to reduce the transition cost, and (3) a zero-knowledge-proof based approach to reduce the verification cost. We further propose and validate that

blockchain application can reduce operational costs (i.e., transaction, transition, and verification costs), and risks (data tampering, system switching, and privacy disclosure risks), and therefore enhance trust among multiple parties. As a result, blockchain application enables efficient and secure data sharing in healthcare insurance.

The rest of this chapter is organized as follows. In Sect. 2, we briefly summarized the fundamental technology of blockchain and existing applications in the insurance industry. In Sect. 3, we described the situation of LTCI and corresponding challenges in China as our research background. The design of our blockchain-based system and the evaluation, including a simulation and application check, were presented in Sect. 4. Future directions and conclusion were elaborated in Sects. 5 and 6, respectively. Finally, the information about the authors was introduced.

2 Literature Review

2.1 Overview of Blockchain Research

The blockchain was originally designed as a public ledger to support the transactions of a first-ever cryptocurrency, Bitcoin. This public ledger is a secure system which effectively resolve the double-spending problems without a third-party authenticator (Nakamoto, 2009; Nofer et al., 2017) by conjointly using the Peer-to-Peer (hereinafter P2P) network and various cryptographic protocols. Elaborately, the P2P network is neither a new phenomenon nor technology, which has been invented to collectively store and share files by a group of devices (Crosby et al., 2016). To record the transactions of cryptocurrency, a secured P2P network is implemented to store a copy of the ledger across multiple anonymous devices. Thus, the P2P network characterizes blockchain technology with a high degree of decentralization. Although P2P network overcomes the limitation and deficiency in the client-service (C/S) structure, the traditional P2P network is yet vulnerable to establish a trustworthy relationship among different anonymous nodes within the network (Khacef & Pujolle, 2019). Thus, a set of cryptographic protocols such as hash functions, symmetric and asymmetric encryption, digital signature, Merkle trees, and smart contract are deployed to encrypt and secure the data storage and exchange. In addition, any changes to the transactional data require the consensus of the majority of the network nodes, which is governed and managed by consensus protocols and algorithms. Given such unique characteristics, the blockchain inherently guarantees that the transactional data is processed in an immutable and transparent way (Yli-Huumo et al., 2016).

In addition to the high degree of security and efficiency, the blockchain, as a programmable artifact, affords considerable promise to integrate with various areas. For instance, financial institutes have attempted to design and implement blockchain-based smart contracts to mitigate the information asymmetry and increase contractibility in an algorithmically automated and conflict-free way (Cong & He, 2019); the merchandisers have also run a trial to use a

blockchain-based system for governing and monitoring the logistics and supply chain (Min, 2019); some rudimental applications are also found in public sector, healthcare, and insurance industry as well though there are few established exemplars to date (Gammon, 2018; Ølnes et al., 2017; Zhao et al., 2016; Zhou et al., 2018).

In the academic literature, there are two general streams of research on blockchain, namely, technical approach and business approach. The former mainly focuses on the design, development, and evaluation or analysis of various blockchain-based systems. For example, Liang et al. (2017) implemented blockchain to synchronize personal health data across different devices for mobile users and found the blockchain-based solutions outperformed the traditional C/S structure in terms of efficiency and security; Zheng et al. (2019) proposed another prototype of the health data sharing systems by jointly using smart devices and blockchain and proved the viability of their proposed system; Zhou et al. (2018) utilized the blockchain to develop a decentralized database to store the medical insurance records and evaluated both technical and economic performance of transactions; Chanson et al. (2019) applied the design science approach to build up a blockchain-based sensor data protection system to prevent the odometer fraud. Despite the technological innovation and novelty in applications, these studies have yet to fully consider the industrial logics or strategic aspects of the blockchain-based artifacts. In other words, the managerial viability of those blockchain-based system or application is still unclear.

The other stream of research is to understand the management and governance of blockchain-related business, which also plays a pivotal role in information systems (hereinafter IS) discipline. For example, Andersen and Bogusz (2019) studied the evolvement of Bitcoin blockchain infrastructure between 2010 and 2016 to exemplarily investigate the theoretical mode of self-organizing; Chong et al. (2019) conducted multiple case studies and derived a theoretical typology of five blockchain-based business models, which affords both the value creation logics and caveats for entrepreneurial viability; Yin et al. (2019) unveiled the blockchain served as an enabler for digital transformation through three initiatives, i.e., issue of cryptocurrency, protection of sensitive information, and elimination of institutional intermediaries, through a case analysis of a large conglomerate. The findings from these works clearly articulated the managerial governance and business value of blockchain. However, the technological components of the blockchain were not comprehensively discussed. In other words, the blockchain was depicted as a "black box," which constrains our understanding of business process due to the influence of technology per se. Thus, there is a call for research to synthesize both technological and business aspects of blockchain in a real case to attain the sociotechnical character of the IS discipline.

2.2 Blockchain for Insurance Industry

Blockchain affords considerable promise to disrupt various industries, including the insurance industry. The insurance industry encounters a series of challenges such as sophisticated compliance issues, prevention of fraud activities, and exchange of fragmented data and transactional records across various parties (Kantur & Bamuleseyo, 2018; Nath, 2016). Such issues result from that the current practice in data management is either inefficient or less secure. Taking the example of the basic model of medical insurance, the relevant information ought to be circulated among hospitals, patients, and insurance companies; however, different parties have their own systems and data schemas, which increases cost of data exchange. More importantly, the insurance companies can only receive certain documents like medical treatment and spending from patients and hospitals, which increases the risks of data tampering. In other words, either patients or hospitals (or even both) may perform fraudulent or collusive behaviors to deceive insurance companies for compensation, if they wish to do so (Zhou et al., 2018). In addition, insurance company also incurs its additional cost of liability assessment to process and handle sensitive and private data.

Although the blockchain is not the end-all-be-all to all challenges encountered by insurance companies, the design of its technological architecture promotes trust, transparency, efficiency, and stability that are needed to address the aforementioned problems in the insurance industry (Zhang et al., 2021). For example, the distributed ledger in blockchain can eliminate the suspicious and duplicated claims by logging each transactional record stored in multiple devices. Such decentralized repositories serve as verifiers to authenticate all historical files and documentation and consequently prohibit the corruption and tampering (Tian, 2017). Besides strengthening the security of the overall process, blockchain can properly manage large amounts of data because the data is recorded with a digitally encrypted fingerprint using date and timestamp. The streamlined data management can support the insurance companies to deliver tailored services and products while assessing risk timelier and more precisely (Raikwar et al., 2018). Moreover, the smart contracts from the blockchain technology increase the capacity of handling transactions and claims through automated process. This contributes to reducing administrative costs and promoting trust among all concerned parties (Kantur & Bamuleseyo, 2018).

Despite the significant potential to disrupt the insurance value chain, there is still a long way to go in overcoming certain challenges. First, the current blockchain projects, excepting cryptocurrencies, are still in the proof-of-concept (POC) stage, lacking viable applications in real- life scenarios in the insurance industry. As such, it is imperative to have concrete evidence to demonstrate the effectiveness of blockchain for health insurance (Sarker et al., 2019). Second, the concern of business privacy is another obstacle hindering the blockchain applications in real-world practice, especially in the insurance industry. Elaborately, there is vast and frequent communication and data exchange among different parties like insurers, reinsures, regulators, hospitals, and clients, among others. On one side, all these parties are typically sensitive to disclose the details of the transactions to unrelated ones; on the

other side, the insurance sector has strong need for data disclosure to complete the authentication. Thus, a novel solution to resolve such a dilemma is necessary.

In this chapter, we design and develop a blockchain-based solution for a real insurance case, i.e., Long-Term Caring Insurance, by collaborating with a leading insurance company in China. Differing from previous studies evaluating the blockchain-based system from a purely technical perspective, we apply a sociotechnical design approach to shed light upon the value of blockchain for the insurance industry. Besides, we creatively apply the zero-knowledge proof, a cryptographic method, to verify the statement with insufficient information, which mitigates the dilemma between privacy and solidity of authentication. We will further explain the details of our design after introducing the research backgrounds and pragmatic challenges.

3 Research Background

3.1 Long-Term Care Insurance Initiative in China

Long-term care is a common issue because people are living longer nowadays. To address such problem, long-term care insurance (LTCI) or similar insurance products are designed and sold in many countries like United States, United Kingdom, Canada, and Germany. Different from the conventional health or life insurance, the LTCI is only used to pay for the costs associated with long-term care, such as Alzheimer's facilities, nursing home, assisted living, and adult daycare, etc. Given the commonweal character of LTCI, only the qualified individuals are allowed to purchase the LTCI.

China is seriously facing the issue of aging society. The foregone one-child policy eventually takes into effect that an adult couple need to provide support for their combined four aging parents. To respond to such societal challenge, Chinese government enacted a new initiative of national LTCI program. This is a cooperative program that government and the qualified individuals, respectively, afford 90% and 10% expense of a commercial insurance for long-term caring. To avoid the vicious competition among insurance companies and the potential monopoly, the government appoints one insurance company as a leading agent and other insurance companies as distributing agents in one city. In other words, for each city, there is only one LTCI product, which is designed and sold by the leading agent. To effectively utilize the existing sales network, the other insurance companies serve as distributing agents to sell this LTCI. To motivate these distributing agents, the government rewards the distributing agents with a fixed amount of compensation per transaction. Besides, considering the practical operation, the government grants the distributing agents to autonomously price its selling LTCI product within a specific range. For the leading agent, it is also authorized to (1) authenticate all claims and documents, such as medical records or reimbursement applications, etc., which are submitted by different parties like hospitals, nursing home, financial institutes, and other distributing agents, and (2) complete the reimbursement for the insured.

Literally, the distributing agents are obligated to collect and authenticate all documentary claims from their own LTCI clients, i.e. those who bought the LTCI should send such files to the local leading agent.

3.2 Current Challenges

In practice, the appointed leading agent encounters several operational challenges due to the current business model of LTCI and the imbalance of regional economic development in China.

The first challenge is how to establish an effective communication mechanism across the isolated and disparate infrastructures owned by different and independent parties to reduce the transaction cost. Since the appointed leading agent is in overall charge of the operation of LTCI in one city, it is necessary to communicate with different parties like local hospitals, nursing homes, and other distributing insurance companies. However, different parties have their own systems with distinctive data schemas. A viable practice is to create Application Programming Interface (hereinafter API) for each system and synchronize the data with the leading agent individually. However, the API-based data exchange is neither trustworthy nor efficient (Yang et al., 2018), whose feasibility is questionable when there is concurrent access by a mass of systems.

The second challenge is how to reduce possible resistance in the implementation. The resistance including two parts, namely the manager resistance and the user resistance. Each participant of LTCI has their own system. The risk and cost of the system switching will lead to the resistance of the managers. Given it is time and energy consuming to get familiar with a new system, users always show strong resistance to system switching. Both resistances will increase the system transition cost. In this regard, it is necessary and important to reduce the possible resistance in the design process.

The last issue refers to privacy protection during data verification, which is especially important in the healthcare domain. Data verification is inevitable in data sharing. Generally, verifiers need to access the plaintext of the data to conduct the verification, which will lead to serious privacy leakage risk. Thus, data verification is a rather challenging task in healthcare since the information is very sensitive. To this end, there is an urgent call for a new approach to complete data verification without showing the plaintext to the verifiers.

3.3 Conceptual Framework of Our Design

To address the abovementioned challenges, we propose a blockchain-based solution. Figure 1 depicts our conceptual framework of trust building by implementing a blockchain-centric data sharing framework. We first identify critical risks and costs that are involved with the efficiency and effectiveness of multi-party data sharing. Then, we propose that trust among multiple parties is an essential antecedent of data

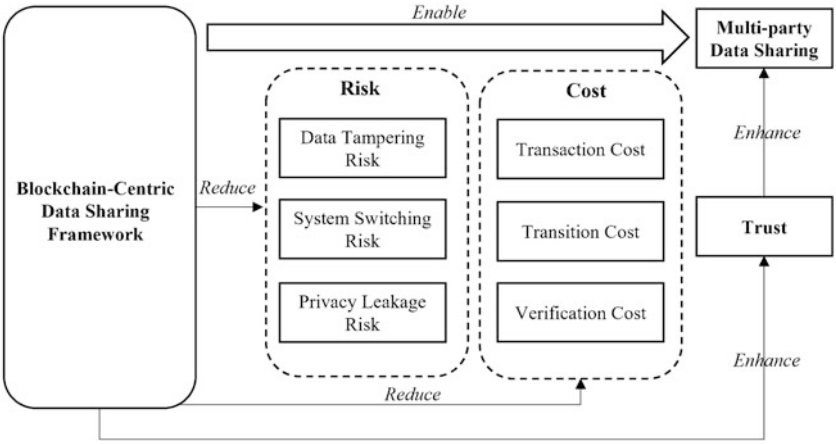


Fig. 1 Conceptual framework of trust building with blockchain in healthcare data sharing system

sharing. In this study, we aim to demonstrate and verify that blockchain application can enable better data sharing among multiple parties when the design reduces operational costs and risks and further enhances trust.

4 System Design and Evaluation

4.1 The Design of Blockchain-Based System

Based on the conceptual framework shown in Fig. 1, we set three prominent goals in our new design. The first goal is to design a system affording an efficient and secure mechanism for communicating among different infrastructures with heterogenous data schema. It is designed to reduce the transaction cost brought by data tampering risk in LTCI. The second goal is to design a layer to enhance the compatibility of new blockchain-based system and existing systems. This additional layer aims to reduce the transition cost along with the system switching risk. The third goal is to conduct the membership proof of diseases without revealing the name of the disease. The membership proof design targets at preventing privacy leakage and at the same time reducing data verification cost in LTCI scenario.

To attain these design goals, we proposed a blockchain-based solution. A middle layer was designed in the form of SDK to connect each participants' existing systems and our novel blockchain-based system to form a trusted network (ATN). Furthermore, smart contracts were also developed to guarantee the truthfulness and timeliness of the uploaded data from each participant. In addition, we complemented this blockchain-based solution with zero-knowledge proof of membership to attain the disease membership proof without full access to the disease information. The framework of our design can be illustrated in Fig. 2. To describe our process clearly,

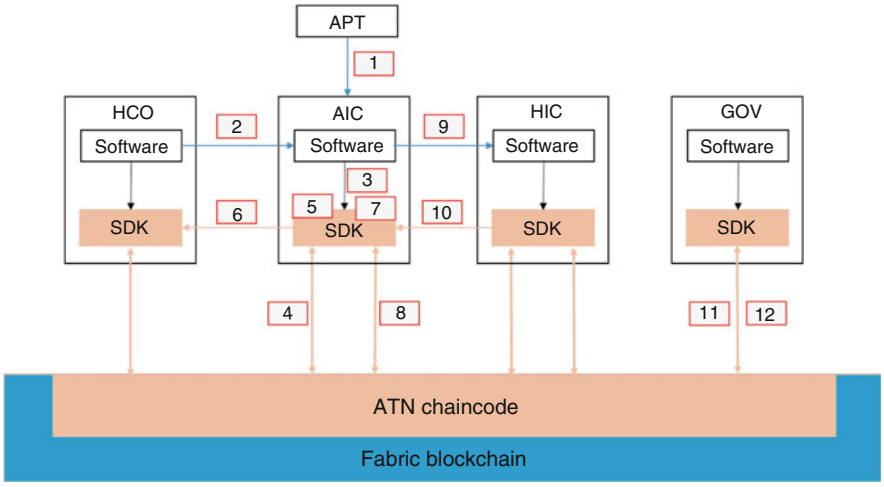


Fig. 2 Illustration of our framework for a single application

we simply choose four typical participants of LTCI, namely applicant (APT), healthcare organization (HCO), agent insurance company (AIC), handling insurance company (HIC) (or we call it leading insurance company, LIC), government (GOV).

The details of the data process and possible interactions can be summarized in 12 steps.

1. An applicant submits an LTCI application (APT) to an agent insurance company (AIC).
2. Since APT can only provide limited untrusted data, AIC needs more precise, trusted data from the healthcare organization (HCO). Thus, AIC calls HCO's application program interfaces (APIs) to access these data. In this step, AIC needs HCO to provide APIs and data access authentication. It has been achieved by existing designs. In our design, we retain the existing systems to reduce the system construction complexity and IT adoption resistance (Azaria et al., 2016). Our design concentrates on what the existing systems cannot do.
3. After a preliminary process of data from APT and HCO, operators of AIC submit the data to its software development kit (SDK). The SDK integrates the primary functions we designed above, including nested hash module, blockchain access module, Merkle tree structure module, identify/authentication module, and zero-knowledge proof module.
4. In traditional API-based system, AIC must trust the data accessed by HCO's API. However, this trust may not be highly reliable due to possible attacks, e.g., man-in-the-middle attack, which refers to a type of cyberattack where attackers relay or even alters an existing conversation or data transfer between two parties—one of the most important reasons for the necessity of deposit. In our design, all participants need to generate data deposits and submit them to the

blockchain. The data deposits can be achieved by the nested hash deposit module embedded in our SDK. In this step, AIC fetches the hash deposit of HCO from the blockchain for further verification.

5. The verification module verifies the hash deposit from the blockchain and the new generated one based on the data collected from HCO's APIs. If they match, then these data are trustworthy. Since every time when we generate hash deposit, we also seal the corresponding digital signature to the deposit. If these hashes do not match, there must be a tampering of the data. Using the corresponding digital signature, it is easy to determine the responsibility.
6. Even AIC has checked that there is no tampering of the data, there may be still doubts about data. For instance, AIC may doubt whether the compensation of a certain disease is proper (i.e., whether it meets the regulation of the policy). However, it is difficult for HCO to offer the detail of certain disease for privacy protection since certain diseases may lead to discrimination to the patient (applicant). In our design, AIC conducts this verification through the zero-knowledge membership proof of the ZKP module.
7. After all necessary checks and verifications, AIC uses its SDK's nested hash deposit module to generate its hash deposit. This hash deposit comes from three parts—data from AIC operations, hash deposit of former dependencies (hash deposit from HCO in this case), and digital signature of AIC.
8. AIC submits its hash deposits to blockchain through SDK's blockchain access module. It is notable that with the expansion of systems (more participants), these nested hash deposit will grow into a Merkle tree. Merkle tree will also help in our later verification and data trace process.
9. AIC submits the order of the applicant to handling insurance company (HIC).
10. In LTCI, authenticated by government, HIC has the right and responsibility to supervise the operations of AIC. For instance, HIC notices that the time consumption of application process for each customer is quite different. Certain discrimination may exist. For instance, HIC doubts that AIC gives priorities for AIC's old customers while delaying the application process of others intentionally. One way to solve this problem is AIC offering its customer list to HIC for double-check. However, it is impossible in real businesses since the customer list is always one of the most precious assets for a firm. In our design, this dilemma can also be solved by the zero-knowledge membership proof.
11. Government plays the role of final supervisor. They need to conduct the audit from time to time. In traditional API-based centralized systems, governments need to audit all the data in all the systems involved. On the one hand, it is extremely resource consuming (time, labor). Moreover, in the audit process, mistakes due to human operation are inevitable, which will make the audit more challenging. On the other hand, the audit process will also lead to serious risk of data leakage. Thus, in traditional design, audit is extremely complicated and cannot be done frequently. In our design, given that we stored the deposit as a Merkle tree structure, governments only need to check the status of the Merkle root to determine the correctness of the whole processes in the flow. It is not only more efficient, but also more accurate.

Table 1 Time cost of detecting data tampering in API-based system and blockchain-based system

No. of parties	API-based system (s)	Blockchain-based system (ms)
1	2.31	0.22
10	3.52	0.30
30	5.45	0.33
50	7.99	0.35
70	10.98	0.37
90	14.22	0.39
110	16.77	0.40

12. When the government finds a certain inconsistency, the mistake can be easily detected through the index of Merkle tree. When the mistake node is detected, it is impossible for the operators to deny it since there is a digital signature in its hash deposit.

To verify the effectiveness of our proposed system, we conducted an experiment to compare the API-based system with our blockchain-based system in detecting a random data tampering through simulation. The evaluation results are shown in Table 1.

In Table 1, the "No. of parties" indicates the number of parties that participate in LTCI and use the system. Apparently, it is more difficult to detect a random data tampering as more parties use the system. From Table 1, it was observed that the blockchain-based system is about 10,000 times faster than the API-based system. Furthermore, the time cost of the API-based system shows obvious increasing trend with the increase of "No. of parties." By comparison, the performance of blockchain-based system is very steady, demonstrating the advantage of expandability of the blockchain-based system. The expandability characteristic is very important in real application especially when the potential market is very large like the LTCI scenario in China.

The feedback of users plays a decisive role in the real application of a system. Thus, we also conducted an applicability check to address the practical and strategic implications. The applicability check includes focus group discussion and in-depth interviews. All participants were employees from insurance companies in the LTCI, including vice president of an insurance company, an IT manager of an insurance company, and four front-end users. The vice president confirmed that the blockchain-based system solved the dilemma of trust in their data sharing. The IT manager stated that the design did not bring extra cost for the transition. Thus, he is willing to switch to the new system since this new system brings convenience for data sharing and verification. Resistance from the manager is relatively small. These front-end users even did not notice that their company have connected to the new system. "I didn't feel any difference," one user said. Hence, the resistance from the end users almost does not exist in our design. According to the demonstration application in two cities, the systems showed great performance both from the

perspective of tampering detection and system popularization according to the feedback of a manager of an insurance company.

4.2 Zero-Knowledge-Membership Proof for Disease Verification

Suppose there is a set of diseases that the patients could apply for special subsidy. However, some members of the diseases in the set may lead to serious discrimination (e.g., AIDS) while others may not. How can an applicant prove that he/she is a patient of certain diseases without revealing the exact disease he/she has?

The encryption technology (e.g., blockchain) holds the promise of privacy protection in data transmission. In many applications, parties involved in one transaction need to conduct certain verification on these transmitted data. For instance, in most cases of DLT (distributed ledger technology like blockchain), all transactions should be validated by all participating nodes. Under these conditions, the data need to be deciphered to plain text so that the verification can be conducted. In this case, whole of the data is revealed to all the participants. In other words, the data is unprotected, and no privacy is protected during the verification process, which leads to a serious crevice to the data security (e.g., privacy protection).

To solve this problem, the protocol of zero-knowledge proof (ZKP) is proposed (Morais et al., 2019). ZKP allows participants to make verifications about the secret data without revealing anything else other than the verifications themselves. With ZKP, all transactions can be validated by all participants without any further information leakage. In our study, we designed a zero-knowledge set membership proof following Morais et al.'s (2019) setting. To conduct zero knowledge set membership proof, the verifier needs to calculate the digital signatures for all the elements in the target set S. These digital signatures are sent to prover. For a message δ, prover also needs to calculate its digital signature and blind this digital signature by raising it to a randomly chosen exponent $v \in \mathbb{Z}_p$. The randomly chosen exponent guarantees that it is computationally infeasible to determine which element was chosen and signed. Finally, prover generates a proof by the pairing, so that the verifier uses bilinearity of the pairing to verify that the message signed by the prover

Table 2 Algorithm of zero knowledge set membership proof

INPUT: Commitment C, set S and g, h
PROPVER INPUT: δ, r such that $\mathrm{C} = g^{\delta}h^{r}$ and $\delta \in \mathrm{S}$
Verifier picks x $\in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$ and sends y $\leftarrow g^{x}$ and $\mathrm{A}_i \leftarrow g^{1/(x+i)}$ for every $i \in S$.
Prover picks $\tau \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$ and sends $V \leftarrow A_{\delta}{}^{\tau}$.
Prover and Verifier run PK $\{(\delta, r, \tau)$: $\mathrm{C} = g^{\delta}h^{r} \wedge V_j = g^{\tau/(x+\delta)}\}$.
Prover picks s, t, $m \in_{\mathrm{R}} \mathbb{Z}_{\mathrm{p}}$ and sends $a \leftarrow e(V, g)^{-s} \cdot e(g, g)^{t}$ and $\mathrm{D} \leftarrow g^{s}h^{m}$.
Verifier sends a random challenge c $\in$R $\mathbb{Z}$p.
Prover sends $z_{\delta} \leftarrow s - \delta c$, $z_{\tau} \leftarrow t - \tau c$ and $z_r = m - \mathrm{r}c$.
Verifier checks that $\mathrm{D} = \mathrm{C}^{c}h^{z_r}g^{z_{\delta}}$ and that $a \leftarrow e(V, g)^{c} \cdot e(V, g)^{-z_{\tau}} \cdot e(g, g)^{z_{\delta}}$.

is indeed one of the elements in S. The process of our design can be illustrated in Table 2.

5 Future Directions

There are many future research opportunities based on this study. First, more advanced technology can be adopted to enhance the capability to deal with emerging complex situations. For instance, in our current design, we utilized zero-knowledge membership proof to verify whether a patient's disease is included in a predefined set. Future research can apply a zero-knowledge range proof to further verify whether a given number is in a certain range (e.g., whether a patient belongs to the low-income group). Nevertheless, zero-knowledge proof, including membership proof and range proof, can only offer simple binary verification. In complex application contexts, certain statistics or even data mining is necessary for the verification process (e.g., verifying the consistencies in documents submitted by different parties). Future research can be conducted to solve this challenge in two directions. The first research direction is to adopt homomorphic encryption to conduct certain calculations on encrypted data. With homomorphic encryption, simple statistics and data mining can be done without revealing the real data (Acar et al., 2018). Since the development of homomorphic encryption is closely related to the mathematical representation of the data and algorithm, homomorphic encryption should be specially designed for an application context. Another research direction is to construct a federated learning framework on the mechanism of parameters sharing and communication. Under the federated learning framework, each party runs data mining models on their own data and shares their parameters synchronously or asynchronously (Li et al., 2020). Since no one needs to share their data with others, and few changes need to be made to existing systems, incorporating federated learning may face weaker resistance in a real application. Second, a field study can be conducted in the future by collaborating with insurance companies, which have adopted the blockchain technology, to further investigate how blockchain technology enables trust building among multiple parties. Although we have compared the time cost of detecting data tampering in the API-based system and the blockchain-based system in this study, a field study can be conducted to further validate the effectiveness of the proposed framework in real practice and to examine the impact of blockchain technology on human behaviors in the healthcare insurance industry.

6 Conclusions

The trend of globalization and digitization calls for closer collaboration among stakeholders, where efficient data sharing is of necessity. However, the trust problem has been a heavy shackle of efficient data sharing. This problem is extremely serious in the healthcare domain, considering the sensitivity of healthcare data. In this chapter, we try to solve this problem from the information technology perspective.

More specifically, we utilize a novel blockchain technology to deal with the trust dilemma in sharing healthcare data in the context of long-term care insurance (LTCI). The blockchain technology provides a new approach to enhancing the security of data in the data sharing among parties without mutual trust. This design could reduce the transaction cost significantly.

Considering that strong resistance may exist in system transition, we designed a middle layer in the form of SDK to connect existing systems and the new blockchain system. The middle layer will facilitate a seamless transition to the new system with minimal adjustments required. Our applicability check verified that the resistance from managers and end users is significantly reduced.

To meet the needs of data verification, we also designed a zero-knowledge-membership proof mode. It allows participants to make verifications about the secret data without revealing anything else other than the verifications themselves. This mode is particularly crucial in healthcare, where safeguarding people's privacy to the utmost degree is of paramount importance. In a nutshell, our chapter demonstrates and validates a viable framework of designing blockchain-centric application to build trust and therefore enable efficient and secure data sharing among multiple parties in healthcare insurance. Our design could reduce transaction cost, transition cost, and data verification cost resulting from various risks in a multi-party collaboration scenario.

References

Andersen, J. V., & Bogusz, C. I. (2019). Self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking. *Journal of the Association for Information Systems, 20*(9), 11. https://doi.org/10.17705/1jais.00566

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur), 51*(4), 1–35. https://doi.org/10.1145/3214303

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. *The 2nd International Conference on Open and Big Data* (pp. 25–30). https://doi.org/10.1109/OBD.2016.11

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems, 20*(9), 1274–1309.

Chong, A. Y. L., Lim, E. T., Hua, X., Zheng, S., & Tan, C. W. (2019). Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems, 20*(9), 9. https://doi.org/10.17705/1jais.00568

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies, 32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation, 2*(6–10), 71.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management, 51*. https://doi.org/10.1016/j.ijinfomgt.2019.10.014

Gammon, K. (2018). Experimenting with blockchain: Can one technology boost both data integrity and patients' pocketbooks? *Nature Medicine, 24*(4), 378–382.

Kantur, H., & Bamuleseyo, C. (2018). *How smart contracts can change the insurance industry: Benefits and challenges of using Blockchain technology*. Master's Thesis, Jönköping International Business School, Jönköping, Sweden, 2018.

Karvounarakis, G., Green, T. J., Ives, Z. G., & Tannen, V. (2013). Collaborative data sharing via update exchange and provenance. *ACM Transactions on Database Systems (TODS), 38*(3), 1–42. https://doi.org/10.1145/2500127

Khacef, K., & Pujolle, G. (2019, March). Secure peer-to-peer communication based on blockchain. In *Workshops of the International Conference on Advanced Information Networking and Applications* (pp. 662–672). Springer. https://doi.org/10.1007/978-3-030-15035-8_64

Kumar, N. (1996). The power of trust in manufacturer-retailer relationships. *Harvard Business Review, 74*(6), 92.

Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. *MIS Quarterly, 29*(3), 461–491. https://doi.org/10.2307/25148692

Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. *Computers & Industrial Engineering, 149*, 106854. https://doi.org/10.1016/j.cie.2020.106854

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications* (pp. 1–5). https://doi.org/10.1109/PIMRC.2017.8292361

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons, 62*(1), 35–45. https://doi.org/10.1016/j.bushor.2018.08.012

Morais, E., Koens, T., Van Wijk, C., & Koren, A. (2019). A survey on zero knowledge range proofs and applications. *SN Applied Sciences, 1*(8), 1–17.

Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system*. https://git.dhimmel.com/bitcoin-whitepaper/

Nath, I. (2016, December). Data exchange platform to fight insurance fraud on blockchain. In *2016 IEEE 16th International Conference on Data Mining Workshops* (pp. 821–825). https://doi.org/10.1109/ICDMW.2016.0121

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Pinjani, P., & Palvia, P. (2013). Trust and knowledge sharing in diverse global virtual teams. *Information & Management, 50*(4), 144–153. https://doi.org/10.1016/j.im.2012.10.002

Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. Y. (2018, February). A blockchain framework for insurance processes. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1–4). https://doi.org/10.1109/NTMS.2018.8328731

Sarker, A., Wuthier, S., & Chang, S. Y. (2019). Anti-withholding reward system to secure blockchain mining pools. In *2019 Crypto Valley Conference on Blockchain Technology,* (pp. 43–46). https://doi.org/10.1109/CVCBT.2019.00004

Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In *2017 International Conference on Service Systems and Service Management* (pp. 1–6). https://doi.org/10.1109/ICSSSM.2017.7996119

Verma, J., & Sinha, A. (2016). Knowledge sharing in cross-functional teams and its antecedents: Role of mutual trust as a moderator. *Journal of Information & Knowledge Management, 15*(3). https://doi.org/10.1142/S0219649216500337

Yang, J., Lu, Z., & Wu, J. (2018). Smart-toy-edge-computing-oriented data exchange based on blockchain. *Journal of Systems Architecture, 87*, 36–48. https://doi.org/10.1016/j.sysarc.2018.05.001

Yin, H. H. S., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). Regulating cryptocurrencies: A supervised machine learning approach to de-anonymizing the Bitcoin blockchain. *Journal of Management Information Systems, 36*(1), 37–73. https://doi.org/10.1080/07421222.2018.1550550

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? – A systematic review. *PLoS One, 11*(10). https://doi.org/10.1371/journal.pone.0163477

Zhang, W., Wei, C. P., Jiang, Q., Peng, C. H., & Zhao, J. L. (2021). Beyond the block: A novel blockchain-based technical model for long-term care insurance. *Journal of Management Information Systems, 38*(2), 374–400. https://doi.org/10.1080/07421222.2021.1912926

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation, 2*(1), 1–7. https://doi.org/10.1186/s40854-016-0049-2

Zheng, X., Sun, S., Mukkamala, R. R., Vatrapu, R., & Ordieres-Meré, J. (2019). Accelerating health data sharing: A solution based on the Internet of Things and distributed ledger technologies. *Journal of Medical Internet Research, 21*(6). https://doi.org/10.2196/13583

Zhou, L., Wang, L., & Sun, Y. (2018). Mistore: A blockchain-based medical insurance storage system. *Journal of Medical Systems, 42*(8), 149. https://doi.org/10.1007/s10916-018-0996-4

Zhu, Y. (2016). Security architecture and key technologies of blockchain. *Journal of Information Security Research, 2*(12), 1090.

Wenping Zhang is an associate professor in School of Information, Renmin University of China. He obtained his Ph.D. in Information Systems from the City University of Hong Kong. His research interests include machine learning, deep learning, interpretable AI, blockchain, and business analytics. His work has been published in INFORMS Journal on Computing, Production and Operations Management, Journal of Management Information Systems, Decision Support Systems and others.

Ruiyun Xu is a Postdoctoral Fellow at the Shenzhen Research Institute of Big Data, Chinese University of Hong Kong (Shenzhen). She received her Ph.D. in Information Systems from the City University of Hong Kong. Her research focuses on financial technology, venture capital, artificial intelligence, design science, and blockchain. Her work has been published in Journal of Management Information Systems.

J. Leon Zhao is a Presidential Chair Professor of Information Systems, a Director of Center on Blockchain and Intelligent Technology, a Co-head of Information Systems and Operations Management, School of Management and Economics, Chinese University of Hong Kong (Shenzhen). He was a Chair Professor (2009–2020) and Head of Information Systems (2009–2015) at the City University of Hong Kong. He holds Ph.D. from Haas School of Business, University of California at Berkeley. Dr. Zhao's current research focuses on blockchain, business intelligence, and FinTech. He has published over three-hundred research papers in journals and conferences, including such journals as Management Science, MIS Quarterly, Information Systems Research, Journal of Management Information Systems, and IEEE/ACM Transactions. He is a Co-editor of Financial Innovation, a Springer Open Access journal, the first SSCI journal in China in the area of finance. He has co-edited over 30 special issues for academic journals including MIS Quarterly, Information Systems Research, and Decision Support Systems. He has chaired about 30 conferences covering Information Systems, Service Sciences, FinTech, and Blockchain. He was awarded IBM Faculty Fellow (2005) and Chang Jiang Scholars Chair Professor of Tsinghua University (2009–2012).

Qiqi Jiang is an associate professor in the Department of Digitalization at Copenhagen Business School. He obtained his Ph.D. in Information Systems from the City University of Hong Kong. His research interests include governance of open-source software development, digital economy, and gamification. His work has been published or forthcoming in MIS Quarterly, Journal of Management Information System, Journal of the Association for Information Systems, The Journal of Strategic Information Systems and others.

Learning to Trust: Exploring the Relationship between Trust and User Experience in Blockchain Systems

Zakir J. Suleman and Victoria L. Lemieux

Abstract

Blockchain can be characterized as a technology that enables social trust between actors. Research on blockchain technology points to the importance of user experience design as providing a foundation trust. What then is the relationship between how users experience blockchain systems and how they may come to trust them? While there is some research exploring how user experiences with blockchain systems influences trust, the relationship between the front-end design of these systems, user engagement, which has been a major focus of user experience design for non-blockchain systems and user trust in blockchain and distributed ledger systems has not explored previously. To address the gap, this study presents original exploratory research on the relationship between user engagement and the user's perception of trustworthiness of a prototype blockchain system that enables patients to share genetic and other biomarker information with healthcare researchers, presenting a theoretical picture of the relationship and design principles to inform future design and research.

1 Introduction

Poor user experience (UX) is widely viewed as a major barrier to, and under researched aspect of, the adoption of blockchain technology. User experience can be defined as a "user's perceptions and responses that result from the use and/or anticipated use of a system, product or service" (ISO, 2019). User experience focuses on the quality of a user's experience with every aspect of a system including the organization, technology, interface, and information (Norman, 2013). The unit of

Z. J. Suleman (✉) · V. L. Lemieux
School of Information, University of British Columbia, Vancouver, B.C, Canada
e-mail: v.lemieux@ubc.ca

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_6

analysis here is the experience of the users, understood as an emergent phenomenon arising from the integration of perception, motivation, action, and cognition into "an inseparable, meaningful whole" (Hazenhal, 2011).

Building on concepts from cognitive science, users and designers are understood to have mental models, sometimes called conceptual models,[1] of how a particular system works (Norman, 2013). Mental models can be defined as "an explanation, usually highly simplified, of how something works. [The model] doesn't have to be complete or even accurate so long as it is useful [to end users]" (Norman, 2013, p. 25). Users develop mental models of a given system based on what they can do with it relative to their goals (affordances), what they can't do with it (constraints), and what is being indicated to them about how to use the system (signifiers) (Norman, 2013). As with any novel emerging technology, users often lack well-defined mental models of how blockchain-based systems work, and in many cases might only come to know a system through their experience of interacting with its user interface.

Designers are understood to have their own conceptual models, in their case about how the system they are designing works and can be used to achieve some goal by end users. Within the context of users' interaction with design artifacts then, designers' conceptual model of the way that a system can be used is conveyed to users through their experience of utilizing the system, mediated through the affordances, constraints, and signifiers of the design of the system (Norman, 2013). This makes it doubly important to better understand the effect that user experience designs have on users' intention to adopt blockchain technology. Indeed, researchers have shown a connection between the quality of user experience with blockchain-based systems and user trust (Voskobojnikov et al., 2021; Sas & Khairuddin, 2017).

For purposes of a discussion of user trust and its relationship to UX, and in keeping with many researchers, we use a definition of trust inspired by Hardin's (2002) notion of trust as "encapsulated interest." In this conceptualization of the term, trust is a three-part relationship that exists when a trustor trusts a trustee with respect to a specific domain of activity (i.e., A trusts B with respect to X). Hinchman (2005, p. 578) further argues that trust "is a species of willed dependence, where the dependence is under appropriate guidance of a counterfactual sensitivity to evidence of untrustworthiness in the trusted." Thus, trust opens the trustor up to taking on some risk, since they are making themselves vulnerable to possible untrustworthiness of the party being trusted.

Much of the literature on trust in technology does not distinguish trust from trustworthiness. We believe a distinction between these two concepts is warranted, since assessment of the trustworthiness of the party being trusted is a critical

[1] Confusingly, the term conceptual model and mental model are used without clarity within Norman's work and within influential design systems like the Apple Human Interaction Guidelines (Norman, 2013). While the idea of mental models pre-date the use of conceptual models by Norman in a design context, I have decided to use the term mental model to refer to the user's model of the system and conceptual model to refer to the model of the system built by designers for clarity.

antecedent and pathway to the formation of trusting relations, i.e. to being in a state of trust. Assessments of trustworthiness are necessary regardless of whether the party, or system, objectively can be trusted. This is not to suggest that the assessment process is an entirely rational cognitive one devoid of affect, only to suggest that knowledge transmission and learning takes place as a foundation for assessments of trustworthiness. Users must be able to learn through the gathering of evidence about the features and operation of a system in order to perceive that the system and its operators are trustworthy and can be trusted. Evidence that the trustee is trustworthy (the counterfactual in Hinchman's (2005) definition of trust) reduces the risk of trusting but such evidence is often uncertain or even unavailable. In the context of information systems, the user interface is probably the single most important channel for the conveyance of the evidence needed by users to assess trustworthiness as a foundation for trust. It is through the user interface, and the user experience that it affords, that users learn about and form judgements about the trustworthiness of a system.

Assessments of trustworthiness take on even greater importance in the context of blockchain technology, as trust is said to be the basis of the technology's *raison d'etre* (See, e.g., Werbach, 2018; Shin, 2019; Lemieux & Feng, 2021; & Lemieux, 2002). Despite that blockchain systems may empirically offer users features that reduce the risk of interacting with untrusted third parties (i.e., as embedded in the notion of "trustless trust" [Werbach, 2019]) or afford trust in the integrity of what is written in the ledger ("ledger trust" [Lemieux, 2002]), most users cannot peer directly into the "deep structure" (Wand & Weber, 1995) of a blockchain-based system to make a determination of its trustworthiness; they must rely only upon their interaction with the system through its user interface to assess the likely behavior of the system and its operators. Consequently, it is essential that UI/UX design of blockchain-based decentralized applications (DApps) and blockchain-based systems concentrates on incorporating features in user interfaces, that provide users with sufficient evidence to make assessments about whether a blockchain-based system is trustworthy, and therefore can be trusted for use.

An important question emerges from the above discussion relating to the relationship between UI/UX and trust in blockchain-based systems: What elements of a UX design influence users' assessment of the trustworthiness of blockchain systems, and which elements lead users to trust the system sufficiently to adopt it for use? The remainder of this chapter presents novel empirical research conducted by the authors aimed at exploring this research question.

2 Methodology

Usability studies are a common research method within the field of Human Computer Interaction and are used in academic and commercial contexts to generate information about the way individuals interact with technology, often for the purpose of improving a specific product or system (Fan et al., 2020). The usability research described in this chapter was conducted as part of a team conducting a

usability study to inform the next iteration of the personal health-related blockchain DApp prototype. The study used multiple methods; specifically, surveys and semi-structured interviews to explore whether the user's experience of engaging with a blockchain-based system for sharing health information affects the user's assessment of the trustworthiness of that system. The term multiple methods is used consciously here in recognition of discussions in the field of mixed methods research and the methodological norms of usability studies. Usability studies regularly incorporate multiple qualitative and quantitative methods based on the context of the research questions, business needs, and situational constraints (Fan et al., 2020; Tarkkanen & Harkke, 2019). The methods were used to elucidate different aspects of phenomena being investigated while providing a holistic understanding and ultimately more grounded recommendations for future designs.

Within user experience there are different normative goals that can be designed for, such as greater accessibility. Recent, work in HCI has centered on *user engagement* as a robust way of structuring and measuring the process of user experience, as well as a goal for design (Doherty & Doherty, 2018). We have adopted it for this research as a useful framework to explore our research question on the relationship between user experience and trust in the use of blockchain systems, hypothesizing that quality of user engagement with the system in some way affects the trust of the user in that system, in the context of the development of perceived trustworthiness.

Measures for trustworthiness were adapted from McKnight et al.'s construct of trust in a specific technology (McKnight et al., 2011). The construct of trust in a specific technology is understood to be predicated on two factors: propensity to trust and institution-based trust. Propensity to trust measures a user's general tendency to be willing to depend on technology and is comprised of faith in general technology (FGT) and trusting stance (TS) (McKnight et al., 2011). Institution-based trust measures the belief that outcomes will be successful due to the presence of supportive situations and structures, and is comprised of structural assurance (SA) and situational normality (SN) (McKnight et al., 2011). A user's propensity to trust has been shown to predict their formation of institution-based trust, which in turn has been shown to predict their trusting beliefs in a specific technology (McKnight et al., 2011). Within McKnight et al.'s work, trusting beliefs in a specific technology are understood to be predictive of future post-adoptive use of a system, and are comprised of the user's assessment of the reliability (RE), helpfulness (HE), and functionality (FUN), of the system (McKnight et al., 2011). Based on McKnight et al.'s work (201), six questions were asked to measure propensity to trust factors, which were included in a pre-session questionnaire. Five questions were asked to measure institution-based trust, and six questions were asked to measure the trusting beliefs of participants. These questions were administered in a post-interaction survey. The questions were rated on a five-point scale from 1 (strongly disagree) to 5 (strongly agree). In addition to the measurements of trust from McKnight, participants were also asked their willingness to share personal information with the system on a 5-point scale from 1 (strongly disagree) to 5 (strongly agree) to measure trust, but rather to measure the assessment of trustworthiness made by participants.

The user engagement scale short form (UES-SF) was used to measure engagement (O'Brien et al., 2018) and administered as part of the post usability study survey. This model of engagement, and its associated User Engagement Scale (O'Brien et al., 2018), has been widely applied and refined for over a decade (O'Brien, 2016b; O'Brien & Toms, 2010; 2013; Doherty & Doherty, 2018). According to this framework, the construct of engagement has four dimensions: aesthetic appeal (AE), perceived usability (PU), reward (RW), and focused attention (FA) (O'Brien, 2016a). The UES-SF comprises 12 questions, three for each factor, that can be used to generate information about the roles of differing factors in the overall experience of a user's engagement (O'Brien et al., 2018). The questions were unchanged from the wording outlined in guidance from O'Brien et al. on administering the scale. The questions were rated on a five-point scale from 1 (strongly disagree) to 5 (strongly agree), apart from the three questions capturing perceived usability which were reverse coded, following guidance from the literature (O'Brien et al., 2018).

It may be asked why this research utilizes validated measurements of both trust and of user engagement, respectively, for quantitative measurement and qualitative analysis but takes an exploratory approach. This approach was chosen because neither of these measurements have been tested in prior work with blockchain technologies. Further, both the theories emphasize the context sensitivity of their respective measures to the specific technology and domain under examination (O'Brien, 2016a; McKnight et al., 2011). Therefore, to assume that these scales can be used deductively within this context would be a methodological error caused by asserting the applicability of these scales to a new area without prior evidence. Instead, these measures have been adopted within this exploratory research to help define an otherwise largely undefined phenomenon.

Non-probabilistic purposive sampling was used to recruit 20 participants using advertisements in REACHBC, a local health-research portal and using the help of a local research firm, Insights West, for recruitment of study participants. Users were asked to participate in usability testing for a new iteration of the software prototype. Before being interviewed, participants were asked to complete a survey, including demographic questions. All research was conducted remotely with participants during the COVID-19 Pandemic, using Zoom and LetsView to mirror and record the users' computer and phone screens. As part of the usability study being conducted by the research team, participants were asked to complete tasks with the system while using a think aloud protocol (Boren & Ramey, 2000). This experience constituted their only interaction with the system prior to data collection. Users were then interviewed by the researchers, and another survey was administered after the interview comprised of items from the UES-SF and items adapted from McKnight et al.'s (2011) work. Data was collected from recorded semi-structured interviews with participants after the tasks from the usability study were completed and from surveys administered to participants after the interviews.

The data analysis took a convergent approach, establishing the existence and features of the phenomenon being explored using quantitative analysis, then using qualitative analysis to help develop nuanced and structured theoretical insights. The

quantitative data collected was analyzed with descriptive and inferential statistics using SPSS statistical software. The interview data collected consisted of video recordings and transcripts of semi-structured post-session interviews conducted with participants. This data was analyzed using NVivo (Online version, release 1.5) qualitative analysis software. Data was also analyzed from the usability test recordings in situations where the topics under discussion were relevant to the goals of this study or were more generative than the content of the interviews themselves. An iterative method of conventional content analysis including negative case analysis and peer debriefing was used to analyze the interview data.

While the scope of this work has been ambitious, it is worth contextualizing the limitations so as to better understand the context in which the findings can be profitably interpreted and built upon. There is an initial methodological question regarding the effect of conducting qualitative data collection from interviews with users about a system *after* the users interact with the system. Another limitation of the methodology is the influence of pre-assigned tasks. In future work, a methodology could attempt to account for this by leaving users to explore the system for a set period of time without restrictions before being interviewed and attempt to improve the reliability of the results through a deductive method of qualitative analysis. Regarding the recruitment of participants, there is a potential for self-selection bias. Specifically, while we attempted to achieve a diversity in education and occupational backgrounds, six participants indicated they were either biomedical researchers or had experience recruiting participants using health-research focused portals. Further, while a variety of steps were taken to ensure the validity of the qualitative analysis, an additional and final step to ensure validity and reliability would have been to ensure intercoder reliability of the qualitative results through the creation of a codebook. This step was deemed to be unnecessary for the goals of the current research, as the current methodology triangulates the findings sufficiently. However, this choice ultimately limits the extent to which the findings of this research can be generalized. Finally, another limitation is the questionable ecological validity of the findings. It is unclear how valid these findings would be in a real-world context, given both the artificial context of the study and the guided interaction that users had through the usability testing. As such, a primary focus of future work would be to begin exploring the applicability of these findings in more naturalistic settings, such as clinical sites.

3 Findings

3.1 Quantitative Result

3.1.1 Measures of Trust and User Engagement

Within this study, quantitative methods were used to establish the existence and quality of a relationship between user assessments of trustworthiness and user engagement. Quantitative data was gathered from surveying participants using the UES-SF and adapted items from McKnight et al.'s (2011) work on trust in a specific

technology. The construct of trust was comprised of three factors (helpfulness, functionality, and reliability), which were measured by two items each. The UES-SF used a five-point rating scale with a total of 12 items. In keeping with guidance on best practices in the use of the UES-SF, the three questions measuring the Perceived Usability factor were reverse coded (O'Brien et al., 2018). Within the UES-SF, there were a total of 12 questions administered to 20 participants for a total of 240 data points. The total engagement scores were calculated by taking the average of each individual's responses, following instructions on using the scale (O'Brien et al., 2018). There were no missing values within the data collected from the UES-SF.

3.1.2 Reliability Analysis

A reliability analysis of the trust and engagement subscales was conducted to ensure they were functioning as intended in the research, given the novel context of their application, and the adaptation of the trust scale. Cronbach's alpha was calculated for propensity to trust ($\alpha = 0.685$, $M = 3.925$, $SD = 0.72$), comprised of two factors (trusting stance and faith in general technology), each consisting of 3 items. Cronbach's alpha was also calculated for institution-based trust ($\alpha = 0.834$, $M = 20.60$, $SD = 3.25$), which is comprised of two factors (situational normality and structural assurance), each composed of two and three items, respectively (see Appendix C). Finally, Cronbach's alpha was calculated for trusting beliefs ($\alpha = 0.835$, $M = 24.45$, $SD = 3.98$) comprised of three factors (reliability, functionality, and helpfulness), each comprised of two items (Table 1).

While there is disagreement about the specific value of Cronbach's alpha that is considered to indicate a sufficient level of consistency; in general, 0.7 is understood to be an acceptable value (Tavakol & Dennick, 2011). The value for propensity to trust fell below that value. In arguing for the sufficient consistency of this value in this novel context, it is worth noting that McKnight's trust in a specific technology construct is an established construct within the MIS field and has been validated in different contexts by McKnight's team, and others (McKnight et al., 2011; Gefen & Reychav, 2014; Söllner et al., 2016). Common practice when addressing a below 0.7 alpha coefficient as a measure of the value of an alpha for a measurement scale is to review the correlations between the scale items and the total score for that scale, and then to remove items that lower the alpha value (Tavakol & Dennick, 2011). However, in this case, there are so few items within each scale that removing items risks compromising the validity of the overall constructs, as indicated by previous research. Without removing scale items, another way to ensure unidimensionality is to calculate the mean inter-item correlation value and measure the distribution of the inter-item correlation values (Clark & Watson, 2016). A mean inter-item correlation value of between 0.15 and 0.50, and a distribution where the majority of the correlation values group close to the mean between 0.15 and 0.50 is understood to indicate unidimensionality (Clark & Watson, 2016). The mean inter-item correlation values were calculated for the propensity to trust factor (see Table 2):

Table 1 Reliability analysis

	α	Mean	SD	Mean of inter-item Correlation	SD of correlation
Trust in specific technology factors					
Propensity to trust	0.685	3.93	0.724	0.388	0.324
Institution-based trust	0.834	4.12	0.902	N/A	N/A
Trust in a specific technology	0.835	4.08	0.954	N/A	N/A
Engagement factors					
Focused attention	0.576	3.65	0.936		
Reward	0.693	4.267	0.634		
Perceived usability	0.866	3.383	1.166		
Aesthetic appeal	0.897	3.367	0.863		

The mean inter-item correlation value was 0.388, and the standard deviation of the correlation matrix was 0.324. As the internal reliability of these was shown to be between 0.15 and 0.5, and the construct of trust in a specific technology has been validated more extensively elsewhere (Söllner et al., 2016), the propensity to trust scales is understood to be sufficiently unidimensional in the context of this research. The score from the trusting beliefs factors was taken as sufficiently representative of the participants' assessment of the trustworthiness of the DApp within this new context. The scores from the factors of trust in a specific technology adapted from the work of McKnight et al. (2011) were then used as a measure of participants' assessment of the trustworthiness of the system in this research and used to explore the relationship between engagement and trustworthiness.

A reliability analysis was also conducted on the four factors from the UES-SF, which are each comprised of three items. Cronbach's alpha was calculated for aesthetic appeal ($\alpha = 0.897$, $M = 3.367$, SD $= 0.863$), perceived usability ($\alpha = 0.866$, $M = 3.383$, $SD = 1.166$), reward ($\alpha = 0.693$, $M = 4.267$, $SD = 0.634$), and focused attention ($\alpha = 0.576$, $M = 3.65$, $SD = 0.936$). However, reward and focused attention fell below an acceptable level of reliability in this context. In this instance, correlation tests were run between the total score for reward and focused attention against the items within their respective subscales. Spearman's rho values for the three focused attention items with the mean value for focused attention were all positive, and moderate to strong (FAQ1 $\rho = 0.660$, FAQ2 $\rho = 0.685$, FAQ3 $\rho = 0.840$). Spearman's rho values for the three reward items with the mean value for reward were also positive, and moderate to strong (RWQ1 $\rho = 0.692$, RWQ2 $\rho = 0.962$, RWQ3 $\rho = 0.684$). As the internal reliability of these measures were all moderate to strong, and the engagement scale has been thoroughly validated in diverse contexts (O'Brien, 2016a), the score from the trusting beliefs factors was taken as sufficiently unidimensional and appropriate to measure the participants' experience of engagement in this context.

Table 2 Propensity to trust correlation matrix

	M (SD)	TSQ1	TSQ2	TSQ3	FGTQ1	FGTQ2	FGTQ3
TSQ1—My typical approach is to trust new technologies until they prove to me that I shouldn't trust them	3.66 (0.816)	1					
TSQ2—I usually trust a technology until it gives me a reason not to trust it	3.80 (0.941)	0.672	1				
TSQ3—I generally give a technology the benefit of the doubt when I first use it	4.06 (0.593)	0.299	0.288	1			
FGTQ1—I believe that most technologies are effective at what they are designed to do	4.20 (0.560)	0.392	0.021	0.368	1		
FGTQ2—A large majority of technologies are excellent	4.13 (0.833)	0.218	0.100	0.293	0.338	1	
FGTQ3—I think most technologies enable me to do what I need to do	4.26 (0.457)	0.067	0.138	0.584	0.122	0.097	1

3.1.3 Descriptive Statistics of the Trustworthiness and Engagement Scales

The average engagement score was 3.37 indicating a moderate overall level of engagement in users' experiences of using the system ($n = 240$) ($SD = 0.988$) (see Table 3). Responses for aesthetic appeal, reward, and focused attention were negatively skewed, with reward having the most dramatic negative skew. Due to both the type of variable (ordinal) and the skewness of the data, the median values are used as the measure of central tendency. Reward had a median value of 4 (somewhat agree) and the lowest standard deviation ($M = 4.27$, $SD = 0.634$), indicating that the majority of participants felt their experience of engaging with the system was characterized by the presence of perceived rewards associated with using the system. Perceived usability had a median value of 4 (somewhat agree) on a 5-point scale, but the largest standard deviation ($M = 3.383$, $SD = 1.166$) as well as a

Table 3 User Engagement Factors

	Median	Mean	Mode	Standard Dev.
Reward	4	4.267	4	0.634
Perceived usability	4	3.383	4	1.166
Aesthetic appeal	3	3.367	3	0.863
Focused attention	4	3.650	4	0.936
Total engagement	4	3.370	4	0.988

Table 4 Trust in specific technology factors

	Median	Mean	Mode	Standard Dev.
Helpfulness	4	3.575	4	1.010
Functionality	4	4.275	5	0.847
Reliability	5	4.375	5	0.807

bimodal distribution, indicating that participants had divergent perceptions of the usability of the system: while some participants felt the system was insufficiently usable, most felt that it was usable. Focused attention had a median value of 4 (somewhat agree), and a standard deviation of 0.936 ($M = 3.65$), indicating that most participants' experience of the system involved an aspect of focused attention, though not strongly. This finding is also perhaps unsurprising, as think aloud protocols like the one used in this study have the potential to negatively impact users' immersion in a system (O'Brien et al., 2020). Aesthetic appeal had a median value of 3 (neither agree nor disagree) on a 5-point scale, indicating that the aesthetic appeal of MYPDx was not a significant factor in participants' experience of using the system ($M = 3.36$, $SD = 0.936$).

In terms of trustworthiness, reliability had the highest median value with 5 (strongly agree) on a 5-point scale, as well as the lowest standard deviation ($M = 4.375$, $SD = 0.807$), indicating that a strong majority of participants perceived the system as reliable, with few outliers (see Table 4). Functionality had a median value of 4 (somewhat agree) on a 5-point scale, indicating that a majority of participants felt that the system was sufficiently functional to guarantee success when using it ($M = 4.275$, $SD = 0.847$). Helpfulness had a median value of 4 (somewhat agree) on a 5-point scale, and the highest standard deviation ($M = 3.575$, $SD = 1.010$), indicating that while a slight majority of participants felt the system offered help when needed, for some participants it was not seen as helpful.

3.1.4 Correlation Between Engagement and Trust

User engagement and trust were first graphed to examine whether they had a monotonic relationship. Because the data being analyzed was ordinal and paired, and there was a monotonic relationship between the variables, Spearman's rank order correlation was used to analyze the correlation between the two variables (total engagement and total trustworthiness) and their respective dimensions (see Table 5). Within the experience of users interacting with the system, overall engagement and

trust had a significant, strongly positive correlation ($\rho = 0.848$). Engagement was most strongly correlated with helpfulness, as a factor of trust in a specific technology ($\rho = 0.804$), then by reliability ($\rho = 0.737$). There was a moderate correlation between engagement and functionality ($\rho = 0.553$). Trust was most strongly correlated with Perceived Usability ($\rho = 0.705$), and moderately correlated with Reward ($\rho = 0.658$) and Aesthetic Appeal ($\rho = 0.626$). Focused Attention ($\rho = 0.510$) and trust, while still moderately correlated, was the weakest relationship.

In addition, an inter-factor correlation matrix was created to summarize the relationships between trust and engagement factors (see Table 5). Notably, helpfulness and perceived usability were found to be strongly correlated ($\rho = 0.706$), as were reliability and reward ($\rho = 0.645$). Finally, correlations between the expressed willingness to share information (the assessment item) and engagement and trust were analyzed. The single item measuring participants' willingness to share information using the system was strongly correlated with their positive assessment of the trust factors, specifically the system's reliability ($\rho = 0.863$) and functionality ($\rho = 0.806$). Of the engagement factors, a willingness to share information was moderately correlated with reward ($\rho = 0.632$) and focused attention ($\rho = 0.601$), but not significantly correlated with aesthetic appeal ($\rho = 0.345$) or perceived usability ($\rho = 0.318$).

Returning to the main research question, we can note firstly that the constructs were understood upon analysis to be operating as intended within a novel context. Secondly, we can note that there was a strong, positive correlation between user assessments of trustworthiness and the engagement of users interacting with this blockchain-based system, based on the quantitative analysis. Of the constructs of trust and engagement used here, perceived usability was strongly correlated with perceived trustworthiness and engagement was strongly correlated with helpfulness. There was also a strong correlation between the way that users perceived the system to be usable and how users felt the system to be helpful. These relationships, as well

Table 5 Trust and engagement correlation matrix

		RW	PU	AE	FA	Overall engagement
RE	Correlation coefficient	0.645**	0.564**	0.393	0.688**	0.737**
	Sig (2-tailed)	0.002	0.01	0.087	0.001	0
FUN	Correlation coefficient	0.432	0.413	0.550*	0.315	0.553*
	Sig (2-tailed)	0.057	0.07	0.012	0.176	0.011
HE	Correlation coefficient	0.578**	0.706**	0.588**	0.365	0.804**
	Sig (2-tailed)	0.008	0.001	0.006	0.114	0
Trust score	Correlation coefficient	0.658**	0.705**	0.626**	0.510*	0.848**
	Sig (2-tailed)	0.002	0.001	0.003	0.022	0

as other significant findings from this analysis, give us an initial picture of the phenomenon we are exploring here.

3.2 Qualitative Results

Where the quantitative results demonstrate the existence and quality of a relationship between the trust and user engagement constructs, qualitative analysis was used to bring theoretically rich descriptions of the relationship being explored. Findings from the quantitative analysis were used to help structure the coding process, which derived inductive themes. These themes were then grouped and structured for internal homogeneity and external heterogeneity. The following themes are most relevant to the relationship between trust and user engagement in the context of the studied system: a general picture of users' conception of trust in blockchain systems, including risk being understood as fundamental to trust and reward as a mitigating factor for trust in risky contexts, and user engagement emerging as a process of learning, with users' experiences of engagement being used as information to inform their assessment of trustworthiness.

3.2.1 Users' Conception of Trust in the Studied System

In order to answer what the relationship between trust and engagement was for users, we begin with an exploration of how users conceived of the potential trustworthiness or untrustworthiness of the system. The common conception that emerged from a strong majority of users was that they felt the system was trustworthy when it had whatever attributes they felt were necessary to mitigate risk, based on specific aspects of the system. Notably, trust was not founded solely (or at all, for a majority of users) on the use of blockchain technology as the basis for the system. An example of this characterization of trust came from participants who specifically spoke to how their experience of the technical architecture of the system contributed to their sense of trust in the system overall. When asked about what made the system trustworthy, P1 said:

> I'm having to scan QR codes that only I would have access to. So that's nice to know. And the two-factor authentication. First, you're just checking your eligibility, and there's an entire process that goes through you [to send your data]. Nobody else can do that. Yeah, I imagine it'd be hard to access (P1).

When asked to elaborate on why my the system would be difficult to access, they provided a metaphor of the QR codes being like a wall: "every QR code you have to scan is like a wall that you have to go through that you only have the key for. If you have your phone and your app, and you've got that sorted (P1)." In this example, the user's experience of using their wallet app to send transactions to the system (by scanning QR codes) is foundational to their sense of the system being trustworthy. The metaphor used here is very telling and speaks to how the user's experience of the system's architecture (mediated through the interface) reinforced their

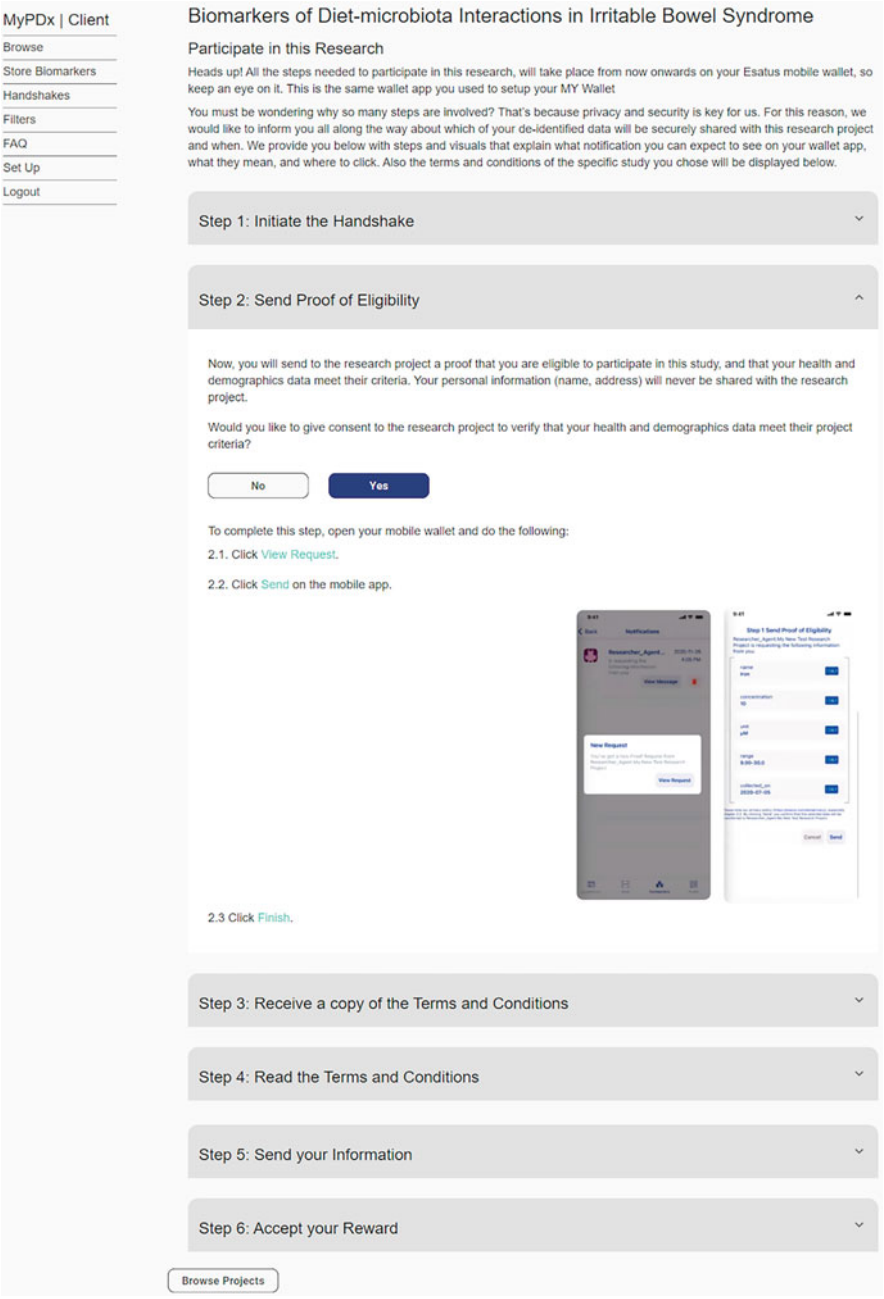


Fig. 1 Handshake Process of the system, using the scanning of QR codes

conceptual model. With this system, users were asked to scan QR codes on the DApp's website with their wallet app to transact with the blockchain used by the system and received notifications when different transactions were completed (see Fig. 1). Notably, the user does not mention blockchain technology as a justification for trust. Instead, their experience of the system's technical architecture helps form a conceptual model of the system connected to technologies with which they are already familiar, which is used as evidence in determining whether or not to trust. The user also spoke of a potential risk that was being mitigated by the architecture of the system, namely that their data might be accessed by other people. Their experience of the system's security and understanding of how to use the system led them to trust that the system could not be accessed by anyone other than them, contributing to their assessment of the system as being trustworthy.

For a majority of users, the assessment of trustworthiness was not ongoing, but instead looked like a one-time decision based on relevant information. Users would engage with the system and, once having learned enough about what they felt were relevant aspects of the system to mitigate risk, made a decision about whether the system sufficiently mitigated risks or presented rewards. As one user said, "I think you need to be initially 100% confident the system is going to work and from there on you're done (P5)." This sentiment was echoed directly by other users: "my thought was once I did it the first time, I was already two feet in. (P14)." While a majority of users assessed the system once, a minority of users also spoke to a desire for more convenience once they felt the system was trustworthy. This was expressed most clearly by one participant:

> Q: Did having to go through all the steps, and having to send each piece of information individually make you feel more in control of the information that you were sharing?
>
> P11: Not really... I think, once you are aware of the biomarkers, when you're ready to just share the information you don't need as much like, when you're ready to go you're good, you know?... the first time, or the first couple times going through it you're getting used to it and you're like 'okay these are the steps involved,' but say you've been using it, and say I've gotten my blood tests done and my markers are changed and I'm sharing my data. After that it'd be a little annoying.

Here the user specifies that there is a difference between using the system for the first time and using the system regularly, where after one is "ready to share the information" the process of sending biomarker information securely by scanning QR codes with the wallet app (as they say, "steps") was less important to the user than then potential lack of convenience over time. Similar sentiments were echoed by other users. For example: "once I start this whole process, I know what it is about. I know that I want to participate in the research and I know that I have to share some information. I just feel like I was checked too many times (P13)." However, it is worth noting that while the majority of users spoke to their assessment of trustworthiness being a one-time assessment, the explicit desire for more convenience after the system was trusted was only expressed by a minority of users.

Throughout these examples then we can see that trust among the users interviewed was conceived of as a one-time assessment, based on their experience with the system, after which a user's priorities in using the system could change. In the case of some users, like P11 above, the priority then became about the relative usability and convenience of using the system, rather than its trustworthiness. They had acquired sufficient evidence from previous interactions to already have determined that the system was trustworthy and feel comfortable placing trust in it.

3.2.2 Risk as Fundamental to Trust

One theme that emerged was the relationship of trust to risk. Almost all interviewees spoke to how they assessed risks and rewards related to using the system as part of their assessment of the system's trustworthiness. In this relationship, in order for the system to be trustworthy it had to mitigate the perceived risks associated with using it. In situations where the system was deemed to be still risky, the system then had to present sufficient rewards to users that they were willing to use the system despite the risk.

Users also spoke to a shared understanding of risk. Almost all users were concerned that the information they were being asked to share through the platform could be used and accessed by unauthorized or malicious actors. We can see the conception of trust as being meaningfully connected to mitigating risk in a comment made by one participant about their assessment of the system as trustworthy:

> Yes . . . .really at the end of the day, what sort of a negative impact would that have if they got a hold of [my biomarker data]? What on earth would they be able to use that info for? Right? So I thought about it, and then, [I thought] 'yeah, I think I'm okay with it.' There are still couple little like, you know, 'should I or should I not?' but, the benefits for me far outweighed the negatives (P20).

We can see in this example how the user clearly located the risk of using the system with unauthorized access to their biological data. The user then deliberated about the potential risks to them of using the system based upon their knowledge of what those risks might be. Finding that they are not aware of any potential negative effects from a scenario in which their data is breached, they then weigh that risk against perceived benefits to make an assessment of the system's trustworthiness. This sentiment was echoed in almost all interviews with participants, indicating a consensus that the system was inherently risky to use, as it required sharing their information online with unknown researchers. Many users also attributed risk to the sensitivity of their biological data.

Overall, the biomarker information participants were asked to share was perceived as particularly risky. As one user put it: "I share my health card number with my doctor. My name, phone number, whatever email, like that's one thing, but I think what freaks me out is putting like biological data online that's really where it takes a shift for me (P2)." This user stated that it was the combination of both biological data and sharing that information digitally that was at issue. We noted a common picture of risk's relation to trust. Users understood that there was risk to

using the system both through sharing information online, and the nature of that information. Users then looked for ways the system mitigated those risks (e.g., by ensuring their security), or offered benefits, as part of their assessment of the system's overall trustworthiness relative to their understanding of their personal risk.

The awareness of risk online came from two sources: firstly, past experiences with the risks of sharing information online, which were connected to assumptions users brought into the session. For example, one user said "[My TurboTax] account was hacked and like the TurboTax people were freaking out and we spent two hours on the phone with them. . . . Other than like the actual official government websites I'm pretty much like assuming that anything can be hacked into (P3)." Secondly, users' awareness of risk came through knowledge they had gained indirectly through other sources: "I think these days, some security data leaks and things like that it's a real issue for people. There's been you know, historical leaks. . . information can leak out quite easily. . .information gets hacked (P3)." Similar pre-session experiences and information about online risks with sharing personal information were noted explicitly by every user in this study and used to inform each individual's assessment of the relative risk of using the system.

Though risk was understood to be inherent to sharing information online for the majority of users, the concern about the severity of that risk depended in part on who the data was shared with. As part of the knowledge that users brought to their assessment, users spoke of various biases toward the likelihood that different kinds of organizations would provide security for their information online. A majority of users were more willing to trust a university, non-profit, or a government rather than a corporation with their information. In some cases, the only organization that was seen to keep data private and safe was the government:

> The second you log into your email, the second you log into Facebook, the second you open an app on your phone, like 99% of the time, your data is just, like, out there. . . . I mean other than, say, like your government, like the [Canada Revenue Agency] website, and you know, doctors' websites, other than those basically any website you log into or any app that you open, you might as well be assuming that everything's out there (P11).

In some cases, the involvement of a corporation was enough to make users want to limit whether they shared their information: "If it's for the greater good. . .testing for information on vaccines. . .then, yes. If it is for let's say towards development of a new drug that will bring profits for the company. . .I don't know if I want to be part of that (P18)." For some users, this was tied explicitly to the ability of insurance companies to base their premiums on biomarker data: "This kind of stuff worries me a bit. . . when all your health data is out there, an insurance company could gain access to your medical records or your information online; it may impact folks getting their life insurance (P7)." In both instances, users indicated that the profit motive of the corporations was an issue for their desire to share their information.

Users adopted different perspectives in the face of this perceived inherent risk to sharing information with the system. In some instances, users spoke to their experience with sharing other forms of personal information online, often with reference to

security enhancing behaviors. For example, one user who had their email hacked before (P11) said, "so I think I would want stronger security settings. That'd be the first thing I look at." It is worth noting in this quote that the user took a pragmatic approach to risk. Having had a pre-existing data breach, their response was not to avoid engaging with services online or sharing information online completely, but instead to assess the system's ability to protect them and speak to what they would need to feel comfortable using it.

Though information sharing may be required to achieve a user's goal with a particular service, almost all users explicitly attempted to assess and mitigate what they felt were inherent risks while maximizing rewards. They did so by engaging in an explicit process of assessment of what information was being collected, and how it was being used and shared, and then implementing behaviors that minimized the perceived risk. Another user summed up the comments of many users, describing the system as "complicated but trustworthy" (P3). The user based their view on features and indicators that mitigate risk. This assessment was also based on the information provided through the user interface, which communicates how the system is being used. However, they note that there is no way for them to know with certainty how the system will use the information, regardless of what the system may tell them. There is no way for them to "look to see where it's being stored," or to see what is being done with their information. Therefore, the user's assessment of trustworthiness is not a statement of certainty about the system, rather the user speaks about trust as a "leap of faith" that they will receive sufficient benefit for "giving up something." The user perceives inherent known and unknown risks to using the system. This structure of assessment was observed in the majority of users, in which risk is either limited, mitigated, or accepted based on the benefits of using the system or the reward received. Once an assessment has been made, the user makes a "leap of faith," where they may still face consequences from using the service, but accept this risk due to their goals, or the reward presented.

3.2.3 Reward

A majority of users spoke about reward or benefits as being a relevant aspect to their assessment of the system. The reward presented by the system was cited as a way of either motivating their data sharing or as a tangential benefit of data sharing, in the context of usability issues and general risk with using the system. The nature of the 'reward' of using the system was almost always connected explicitly to the way the system offered monetary compensation to users for the contribution of their data, rather than the quality of their experience, as reward in itself and as characterized in the UES-SF.

Some users were more explicit than others about needing to be compensated: "Once you go in there, 100 bucks to like share information and not have to do anything? Yeah, that's pretty good (P15)." In other cases, the reward was seen as a benefit to having already shared the information with the testing company by sharing a blood sample: "It's a pretty easy reward for all you're doing. All you're doing is giving permission for researchers to use your data, you know? Once you've got the information it's there to be utilized. If somebody wants to pay me for it, great (P17)."

For some users, the role of reward was even more explicit when talking about sharing their biomarker information. In the case of one user who had indicated they trusted the system: "That's why I said, you know, repeatedly, that I wouldn't do this without any incentives, right? Just for fun? I wouldn't do it (P13)." This user, in particular, cited usability issues as a problem with the system as a reason why they would need to be further motivated to use the system.

In a minority of cases, participants spoke to how the benefit to society or individuals currently affected by diseases without treatment regimens was seen as a "benefit" or "kickback" for users, which is largely consistent with the findings of Lu et al. (2020) as an earlier study completed as part of the larger research project of which this study forms a part. As one user said, "There's definitely that little kickback that helps, but you know from a community perspective, how are we going to fight all these illnesses that we have? We need people to volunteer to share data or share their experiences, right? (P7)." In these minority of cases, monetary compensation was not mentioned at all, with the social good of sharing information seeming to take the place of reward as a motivation for signing up for a study to share their information. For example, one user stated:

> I like the idea, just like doing this, you know? Being able to help with research for things are [sic] going to make things better, hopefully. . .whether it's a medication or some sort of a program that can help, you know, deal with different health issues. That type of a thing. . . . I just I like the idea of, you know, the altruistic aspect of it right, helping society to better [understand] something. So those are the benefits to me (P20).

However, even though compensation was not mentioned by the user, the social benefit of their information was also understood as a benefit of using the system, rather than strictly speaking as a way in which the experience of using the system was inherently rewarding. We can see from these examples that the picture of how the system presented rewards was understood by users as distinct from whether their experience of using the system itself was rewarding. These social rewards, like the monetary rewards, were discussed in reference to the perceived risks of using the system. The evaluation of what constituted a risk and reward was explicitly connected by users with past experiences with technology, perceptions of security online, attitudes toward different kinds of actors that might be able to access the information, and their own value systems.

3.2.4 Engagement as Learning Process

Echoing the literature on engagement, a theme that emerged from the interviews was the role of engagement both as a process and a product relevant to users' assessments of the system's trustworthiness. A majority of users indicated that they learned through engaging with the system, either explicitly or implicitly. As one user stated: "It was kind of like connecting the dots a little bit. . .wasn't as clear the first time, but second or third time we were kind of repeating the things [and] it did get a lot easier (P3)." A good example of the process of learning in this system comes from one user who explicitly spoke about their confusion concerning how what they were being

asked to do connected with the usability testing session: "It was very obvious what I needed to do with the directions that were provided. But I guess like, overall, the sort of purpose of it, you know, clicking on entering these codes. . .Yeah, that's confusing (P1)." Later in the same session, the user spoke to their process of learning: "It took me a bit of time to realize that when I click "yes" on the screen here [on the computer] that it sort of sends a request to my app [on my phone]. That wasn't quite intuitive (P1)." By the end of the session, the same user was able to speak clearly to the conceptual model of the system, and used it as a rationale for their assessment of the system's trustworthiness when asked about the potential for the system to be "hacked": "I think given there's such like, strong linkage, for lack of a better term, between what's on the web, and you know, how permissions are provided, or the data is shared through the app (P1)." In this example, the user clearly spoke to a process of learning how the system worked, through using the mobile wallet app to send information with the help of the web browser. They then applied that knowledge to speak to their assessment of the trustworthiness of the system. It is also worth noting that the user here is actively speaking about how the system mitigates what they see as potential risks. Users also gained a sense of confidence in the purpose and outcome of what they were being asked to do with the system. As P1 (quoted above) said: "Well, I literally saw what happens in what order so now I'm comfortable with it. I see what happened. . . there's no surprises." The confidence expressed by P1 presents an example of the process of learning mirrored by the majority of participants, where they moved from confusion to confidence through learning by engaging with the system. Echoing the literature on engagement, other users mentioned that the ability to experiment with and "play" with the system was essential to their comfort with the system:

> I found it really helpful. . .my only concern was that you know I could play with this all day long. . .I was going to mention that at one point: please don't tell me that there's ever a time constraint on. . .your ability to you know be in the system. Because I think that would frustrate people. . .if it's something that you know they can [do] on their own time, get familiar with and get comfortable with and navigate through. . .familiarize themselves with it, I think it's going to go like gangbusters (P6).

This user speaks clearly to how their ability to experiment with different parts of the system helped them to "familiarize" themselves and "get comfortable with" the system. This kind of deep structure use is understood as a part of engagement within the literature. While this user was the only user to speak of "play" as part of their process of learning, the comments about how using the system helped them to form an image of how the system works echo the majority of participants. As demonstrated above, for a majority of users, engagement was the process by which they learned about the structures of the system and gathered evidence that was relevant to their assessments of the trustworthiness of the system.

To a certain extent this finding is intuitive, as users were asked to complete tasks with a system they had never seen before without other sources of information than what the system presented. Further, the relationship between engagement and learning has been explored in eLearning settings with reference to how specific

populations and designs influence learning (O'Brien, 2016b; Vail et al., 2015). The relationship between engagement and learning has also been explored within the field of cognitive psychology (Wiebe & Sharek, 2016). For example, Cognitive Load Theory posits that a primary goal of information processing is the "activation and modification of existing schemas for learning" (Wiebe & Sharek, 2016, p. 58), and that attention is limited and selective, such that "While the learner has made the higher-level decision to engage in a learning task, the design of the learning environment will heavily influence what specifically is attended to over the arc of a learning session" (Wiebe & Sharek, 2016, p. 58). Discussion of the specifics of this process and its relationship to the design of this system however is beyond the scope of these findings and this research.

3.2.5 Experience of Engagement as Information for Assessment

Within the interviews, users cited their experience of how well the system engaged them as a primary source of information for their assessment of the system's trustworthiness. Following the literature on engagement, this theme broadly aligns with the understanding of engagement as a product of user experience.

For a majority of users, relevant information was derived from users' experiences with different features that engaged them in a relevant way to their users' assessment of trustworthiness. For example, many users cited their perceptions of the system's usability, specifically, experiences of interactivity and feedback, as a reason the system was secure. For these users, the metaphor of having experienced "steps" or "checkpoints" was used as a rationale for the system's security. As one user said:

> The way that it's been set up to keep things like quite safe. . .going to your phone and then [information] being sent to [it] and, like you kind of make these calls and there's a lot of checkpoints. I think that really helps and making it feel like a safe tool (P2).

For this user, the experience of feedback (or perhaps friction) gave them a sense of control over the system and therefore over their information. The "steps" also gave users a clearer sense of the technical architecture of the overall system, through helping develop a conceptual model. For example, the user quoted above spoke to how they felt their data was being minimized through the technical architecture of the system: "I think, especially because of all of the steps that I've had to go through it's like okay, yeah, they really are getting this one bit (P2)." The ability of this user to identify that their data was being minimized by design speaks to the way in which users' experiences of the system's usability, mediated through the interface, became an important source of information for users about the goals and structure of the system as a whole. It is also worth noting here that this sense of security, that researchers are "getting this one bit" of the users' information, comes not from any knowledge of blockchain technology or the specific type of cryptography used to protect their data, but rather from information gained from their experience of engagement with the interface of the system.

Overall, the results of our research revealed that users relied upon their experience of engagement with the system as a source of information as to how the system

mitigated risk. This took the form primarily of observations of users about the system's perceived usability, specifically feedback, interactivity, and friction. Other aspects of user engagement from the literature were relevant to users' assessments of trustworthiness, including reward and aesthetic appeal. We can build upon the strong positive correlation between trust and user engagement with the following: trust was understood by users to be meaningfully related to risk, such that the system had to either mitigate risk and/or present rewards to be trusted. Users spoke to a common understanding of risk, namely that their biological information would be accessed by an unauthorized actor. Sharing information online, and specifically sharing biological information online were understood to be fundamentally a risky behavior by almost all users. Users were also receptive to rewards offered for using the system and taking that risk, using them to justify relying upon the system in instances where they felt the system was insufficiently trustworthy. In every interview, users were observed to engage in an explicit process of assessing the system's trustworthiness based on their understanding of the risks of using the system, how the system mitigated those risks, and how it presented rewards that incentivized use. A common picture of the relationship between engagement and trust emerged, whereby engagement was both a process by which users gathered relevant evidence about the trustworthiness of the system. Building off the quantitative findings, a majority of users' experience of the system's perceived usability, as a factor of engagement, was cited by users as a reason for their assessment of the system as trustworthy.

4 Design Implications

It is a common practice within HCI scholarship to derive design implications as a way of making insights from research actionable for future designers. The primary audience for the recommendations below is designers and researchers exploring how to develop new and trustworthy technologies within the area of health-related blockchain systems more generally (with the caveat that the relationship between the findings of this research and other blockchain systems has yet to be empirically demonstrated).

4.1 The User's Conceptual Model of the Entire System Is Essential to Trust

When it comes to trusting a new system, users look to learn about a new system to see whether it is trustworthy. Explicitly supporting the development of a conceptual model through both the information conveyed to users and the experience provided to users may help users make better sense of this new type of system.

4.2 Designing for Engagement May Support Trust

While causation has yet to be proven, there is a strong correlation between users' assessments of the trustworthiness of a system and their engagement with a system. This means that designing for trust may entail designing for engagement. The ability of a new system to convince users that it is trustworthy relies on its ability to show users relevant features that mitigate risk and present sufficient reward. Engagement is an important process and source of information for the making of such assessments by users. In addition, treating engagement as a design outcome may also lead to an improved experience for users.

4.3 Balance Information Asymmetries

When it comes to trusting a blockchain system, users are in an inherent information asymmetry with the system and its operators. While users may have relevant design or technology metaphors to draw upon in interacting with a blockchain-based system, these metaphors may do more to confuse than inform. Therefore, a design goal should be to explicitly provide users with as much information as they need to assess the system's trustworthiness.

4.4 Support Learning through Feedback

Users may learn through a process of engaging with the system. The way users perceive the usability of the system and, specifically, experiences that give users a sense of feedback and control, help users to gain information about the space of permissible action for them and other users. This information is important for users' assessment of the system's trustworthiness. Design elements and sections should carefully consider where it may be appropriate to communicate key ideas about the system through feedback or even friction.

4.5 Focus on Information Architecture

When encountering a new technology, or an unfamiliar modality, IA is a key place where users find information and use it to make sense of their new digital context. The end goal for users is to develop a conceptual, or mental model, of the unseen aspects of the system, such that they can make a reasonable assessment as to its trustworthiness. Focusing on creating a coherent, logical, and approachable means of representing a system's IA for users should be prioritized to help users develop a conceptual model within unfamiliar systems.

4.6 Ensure that the System Is Helpful in an Accessible, Clear Way

Content, copy, and images are primary avenues for communication about an unknown type of system. Language should be clear, accessible, and informative without being overwhelming. Images should be integrated thoughtfully in places where they have the greatest explanatory power. Conducting content audits or testing language with lay users may be useful avenues for future designs.

4.7 Give Users Ample Organizational Assurances

Users are looking to learn more about the motives, incentives, and capabilities of others they may interact with through a platform. Clearly speaking to the incentives, actions, restrictions, and oversight placed on other actors by the system may help users to assess whether those other actors are trustworthy. Logos, third party links, and other markers of legitimacy that allow users to corroborate the information presented from other sources may also be relevant.

4.8 Offer Rewarding Experiences

Reward is a relevant part of user's assessments of trustworthiness and can help motivate users to continue to use a system as part of their assessments of risk and rewards of system use. Careful consideration of where and what kind of rewards and rewarding experiences is being presented to users should be a focus of future designs.

5 Conclusions

This research contributes design implications and an initial theoretical exploration of the relationship between trust and user engagement to the emerging area of the study of blockchain systems. In so doing, it argues for the importance of the design of systems, specifically the front-end design of systems, to user's perceptions of the technologies they use. Unlike the vision of Bitcoin users outlined by Satoshi Nakamoto (2008), users of current consumer facing blockchain technologies, seeking to take advantage of the benefits of this social technology, are not experts. Many may have never heard of blockchain technology before, much less understand how it works in a way to be able to verify their transactions on the ledger. This means that for many users, the most important information that will guide their decision to trust, and ultimately to use, a blockchain system is conveyed through their experience of the front-end of that system. Designing for engagement, then, emerges within this work as one way to create positive user experiences that have the potential to influence the way users assess the trustworthiness of new blockchain systems.

The research offers several contributions that while limited in scope are potentially relevant to multiple fields and endeavors. First and foremost, this work expands on the blockchain literature by conducting a usability study with users of a blockchain system and is the first study on the relationship between trust and engagement in blockchain systems (to the best of the authors' knowledge). Importantly, it also studies the design of a non-crypto-focused blockchain system, and focuses on the effect of the front-end design, rather than the effect of the solution architecture, on trust. This work also creates theoretical connections between the relationship of engagement and trust between the theoretical frameworks of McKnight et al. (2011) and O'Brien et al. (2018), and is (to the authors' knowledge) the first research to explore this intersection. In addition, this work expands the application of the UES-SF and the process model of user engagement to a new domain (blockchain systems) further demonstrating its generalizability. This work also contributes limited empirical support for emerging work by Lemieux, though further work is needed to validate Lemieux and Feng's (2021) work on trust and blockchain technology, as this research focuses only on one aspect of their model, namely user trust. This work also expands on McKnight et al.'s (2011) theory of trust in a specific technology adding conceptual clarity to this theoretical strand within the MIS literature. Finally, this work contributes to the small body of work on the UX design of blockchain systems, building on work by Sas and Khairuddin (2017), Voskobojnikov et al. (2021), Eskandari et al. (2018), and Zavolokina et al. (2020) and presents design implications to guide future work by researchers and designers. While there is still a need to establish the validity and generalizability of this work in a larger context, as the findings here are exploratory, once additional more confirmatory research has been taken, we hope this work can be generative in many directions.

References

Boren, T., & Ramey, J. (2000). Thinking aloud: Reconciling theory and practice. *IEEE Transactions on Professional Communication, 43*(3), 261–278. https://doi.org/10.1109/47.867942

Clark, L. A., & Watson, D. (2016). Constructing validity: Basic issues in objective scale development. In A. E. Kazdin (Ed.), *Methodological issues and strategies in clinical research* (pp. 187–203). American Psychological Association. https://doi.org/10.1037/14805-012

Doherty, K., & Doherty, G. (2018). Engagement in HCI: Conception, theory and measurement. *ACM Computing Surveys, 51*(5), 99. https://doi.org/10.1145/3234149

Eskandari, S., Clark, J., Barrera, D., & Stobert, E. (2018). *A first look at the usability of bitcoin key management*. arXiv preprint arXiv:1802.04351.

Fan, M., Shi, S., & Truong, K. N. (2020). Practices and challenges of using think-aloud protocols in industry: An international survey. *Journal of Usability Studies, 15*(2).

Gefen, D., & Reychav, I. (2014). Why trustworthiness in an IT vendor is important even after the vendor left: IT is accepting the message and not just the messenger that is important. *Omega, 44*, 111–125. https://doi.org/10.1016/j.omega.2013.11.002

Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.

Hinchman, E. S. (2005). Telling as inviting to trust. *Philosophy and Phenomenological Research, 70*(3), 562–587.

Hazenhal, M. (2011). *User experience and experience design*. Retrieved December 17, 2020, from https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/user-experience-and-experience-design

ISO DIS 9241–210:2019 (2019). *Ergonomics of human system interaction–Part 210: Human-centered design for interactive systems*. International Organization for Standardization (ISO).

Lemieux, V. L. (2002). *Searching for trust: Blockchain Technology in an age of disinformation*. Cambridge University Press.

Lu, C., Batista, D., Hamouda, H., & Lemieux, V. (2020). Consumers' intentions to adopt blockchain-based personal health records and data sharing: Focus group study. *JMIR formative research, 4*(11), e21995.

Lemieux, V. L., & Feng, C. (2021). Conclusion: Theorizing from multidisciplinary perspectives on the Design of Blockchain and Distributed Ledger Systems (part 2). In V. L. Lemieux & C. Feng (Eds.), *Building decentralized trust: Multidisciplinary perspectives on the Design of Blockchains and Distributed Ledgers* (pp. 129–163). Springer International Publishing. https://doi.org/10.1007/978-3-030-54414-0_7

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on management information systems (TMIS), 2*(2), 1–25.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review, 21260*.

Norman, D. (2013). *The design of everyday things: Revised and Expanded Edition*. Basic Books. http://ebookcentral.proquest.com/lib/ubc/detail.action?docID=1167019

O'Brien, H. (2016a). Theoretical perspectives on user engagement. In H. O'Brien & P. Cairns (Eds.), *Why engagement matters: Cross-disciplinary perspectives of user engagement in digital media* (pp. 1–26). Springer International Publishing. https://doi.org/10.1007/978-3-319-27446-1_1

O'Brien, H. (2016b). Translating theory into methodological practice. In H. O'Brien & P. Cairns (Eds.), *Why engagement matters: Cross-disciplinary perspectives of user engagement in digital media* (pp. 27–52). Springer International Publishing. https://doi.org/10.1007/978-3-319-27446-1_1

O'Brien, H. L., Cairns, P., & Hall, M. (2018). A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. *International Journal of Human-Computer Studies, 112*, 28–39. https://doi.org/10.1016/j.ijhcs.2018.01.004

O'Brien, H. L., Morton, E., Kampen, A., Barnes, S. J., & Michalak, E. E. (2020). Beyond clicks and downloads: A call for a more comprehensive approach to measuring mobile-health app engagement. *BJPsych Open, 6*(5), e86. https://doi.org/10.1192/bjo.2020.72

O'Brien, H. L., & Toms, E. G. (2010). The development and evaluation of a survey to measure user engagement. *Journal of the American Society for Information Science and Technology, 61*(1), 50–69. https://doi.org/10.1002/asi.21229

O'Brien, H. L., & Toms, E. G. (2013). Examining the generalizability of the user engagement scale (UES) in exploratory search. *Information Processing & Management, 49*(5), 1092–1107. https://doi.org/10.1016/j.ipm.2012.08.005

Sas, C., & Khairuddin, I. E. (2017). Design for trust: An exploration of the challenges and opportunities of bitcoin users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 6499–6510*. https://doi.org/10.1145/3025453.3025886

Söllner, M., Benbasat, I., Gefen, D., Leimeister, J. M., & Pavlou, P. A. (2016). Trust. In A. Bush & A. Rai (Eds.), *MIS quarterly research curations*. https://doi.org/10.25300/10312016

Shin, D. D. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics, 45*, 101278.

Tarkkanen, K., & Harkke, V. (2019). Scope of usability tests in IS development. *AIS Transactions on Human-Computer Interaction, 11*(3), 136–156.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53.

Vail, A. K., Boyer, K. E., Wiebe, E. N., & Lester, J. C. (2015). The Mars and Venus effect: The influence of user gender on the effectiveness of adaptive task support. In F. Ricci, K. Bontcheva, O. Conlan, & S. Lawless (Eds.), *User modeling, adaptation and personalization* (pp. 265–276). Springer International Publishing. https://doi.org/10.1007/978-3-319-20267-9_22

Voskobojnikov, A., Wiese, O., Koushki, M. M., Roth, V., & Beznosov, K. (2021). *The U in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets* (p. 22).

Wand, Y., & Weber, R. (1995). On the deep structure of information systems. *Information Systems Journal, 5*(3), 203–223. https://doi.org/10.1111/j.1365-2575.1995.tb00108.x

Wiebe, E., & Sharek, D. (2016). ELearning. In H. O'Brien & P. Cairns (Eds.), *Why engagement matters: Cross-disciplinary perspectives of user engagement in digital media* (pp. 53–79). Springer International Publishing. https://doi.org/10.1007/978-3-319-27446-1_3

Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.

Werbach, K. (2019). Summary: Blockchain, the rise of trustless trust? *Wharton PPI B-School for Public Policy Seminar Summaries*. https://repository.upenn.edu/cgi/viewcontent.cgi?article=1002&context=pennwhartonppi_bschool

Zavolokina, L., Ziolkowski, R., Bauer, I., & Schwabe, G. (2020). Management, governance and value creation in a blockchain consortium. *MIS Quarterly Executive, 19*(1), 1–17.

Zakir Jamal Suleman is a 2022 graduate of the Masters in Library and Information Science Program at the University of British Columbia. His research interests sit at the intersection of value-sensitive design, human-computer interaction, assemblage theory, and radical democracy. He is deeply interested in the ways technology (as co-constitutive of modern human life) enables, shapes, and influences the systems that everyday people live within and struggle to improve. He currently works as a Service Designer, leading primary research projects and co-designing innovative peer-based solutions to problems faced by individuals at the intersection of extreme poverty and systemic discrimination. He is also the co-founder of CaseTalk, a legal technology start up that leverages generative AI to improve access to justice. He has worked with partners from Microsoft Research to investigate productivity tools for knowledge workers, led consultations for the Canadian federal government on innovation in refugee settlement, and conducted research on equity best practices in North American Science Faculties. He is an ALA Calloway Scholar, an ARL Kaleidoscope Scholar, and the recipient of the Mitacs Accelerate scholarship.

Victoria Louise Lemieux is a Professor of Archival Science at the University of British Columbia School of Information. She is also a Founder of Blockchain@UBC, the University of British Columbia's Blockchain research and education cluster, a Sauder School of Business Distinguished Scholar, and a Faculty Associate of the Institute for Computing, Information and Cognitive Systems at UBC. Her interests include risk to the availability of trustworthy records through an archival science theoretic lens, in particular in blockchain record keeping systems, and how these risks impact upon transparency, financial stability, public accountability, and human rights. Dr. Lemieux has won several awards for her research and contributions to the field of archives, records management, and cybersecurity, including receiving in 2015, the Emmett Leahy Award for contributions to the field of records management and a World Bank Big Data Innovation Award, and in 2020 a Blockchain Ecosystem Leadership Award and recognition as one of Canada's Top 20 Women in Cyber Security in 2020 by IT World. Her latest publications including *Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers* (Springer, 2021) and *Searching for Trust: Blockchain in an Age of Disinformation* (Cambridge University Press, 2022).

Design and Implementation Considerations for Blockchain for Health Records

Prashant Khambekar

Abstract

This chapter provides the motivation for using blockchain-based systems for health records as the currently prevalent electronic health records are inadequate for providing complete care and a smooth experience. The organization of such systems is discussed for developers intending to proceed on this path. Real examples from multiple such systems indicate that the challenges faced by developers in creating and deploying successful systems are not trivial. The issues are described here in depth and the corresponding solutions are discussed.

1 Introduction

Health records are being maintained in electronic systems for many years now. So, why is blockchain for health records desirable?

Consider a simple patient situation. Patient Paolo is sent by his family dentist to get one of his molars examined by an endodontist for a possible root canal. Paolo has to provide all the dental history to the endodontist and inform about the tolerance to local and general anesthesia as well as allergies to certain classes of medicines. The next year Paolo is referred to a periodontist for an unrelated gum problem and Paolo again has to provide the dental history, the anesthesia information, and the allergy information. This problem arises because every practitioner keeps their patient information in their own silo. Due to lapses in memory, and possibly not realizing the importance of all relevant history, Paolo only provides some of the information. Paolo thus faces the unnecessary risk of side effects.

P. Khambekar (✉)
Harbinger Systems, Philadelphia, PA, USA
e-mail: prashant.khambekar@harbingergroup.com

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_7

Consider a slightly more complicated situation. Patricia complains about discomfort in her feet. She undergoes surgery in a hospital and is provided with a cast. When she is discharged from the hospital, she has to continue the pain medication. At the same time, she needs to continue to be seen by her family physician for her chronic, low-impact problems. If the family physician does not get the complete picture of her medication and whether it has affected her overall health, there can be unnecessary complications. Soon, Patricia must start physiotherapy for the foot condition and the physiotherapist needs to see her X-ray images. So, Patricia has to remember to carry to the physiotherapist the image CD provided by the hospital to her. For the proper continuity of care, accurate health data records need to be shared across doctors.

Health records are related to one person, but they are locked into siloes. And for proper care by a collection of doctors, the complete sharing of information is desired. In some regions of the world, doctors do not trust the accuracy of the data residing with other physicians and health systems. A blockchain can provide the confidence that the data is accurate and is neither missing nor faked. The trust enabled by the blockchain allows physicians to share data (Peral et al., 2020; Azaria et al., 2016).

HL7 is a mechanism for sharing health record data from one party to another. DICOM is a standard for health image data which enables the sharing of health images. These form the basis of the transfer of health data across systems. However, they do not ensure continuity of care and complete care because not everyone shares the information. Doctors and hospitals maintain siloes of information and updates may not be shared leading to un-synchronized siloes. There is no guarantee that data is not faked. And even though health data is related to one person, there can be multiple identification keys—sometimes within a single system—leading to a mess. In contrast, the trust enabled by the blockchain encourages the sharing of health data.

A few companies have come forth with blockchain-based storage of health records. (Confidentiality agreements restrict disclosing the names of customer companies and fairness prevents the mention of other companies, but they can be found by searching on the Internet.) Patients can view their records. Doctors can view the records to which patients have given them permission to read. Patients can either add new records or permit the import of health records from EHRs and similar systems. Data can be shared with other doctors for continuity of care or expert opinions or second opinions. When such data is accumulated and available, medical research groups, pharmaceutical companies, and clinical research groups are interested in studying the data for understanding diseases and for developing new therapies. (Some use cases are given in Sect. 3 below.) This data can be either the raw data of individual records or it could be aggregated, anonymized data. Typically, patients need to permit part or the whole of their data to be provided to such entities. The users of such a system are patients, doctors, and research organizations along with a few administrators for overseeing the smooth sharing of data.

This chapter covers the organization of blockchain-based health record systems and the issues faced by developers and entrepreneurs. Section 2 covers the basic structure of the system. Section 3 starts off with simple use cases and how to map that to the blockchain system, and then moves to more complicated use cases. The rest of the sections address issues in order of simple to complex. Section 4 talks

about how the systems are organized based on the peculiarities of the blockchain concept. Section 5 addresses which blockchain to use out of the available blockchains or whether one can create a blockchain from scratch. Section 6 talks about the overall user experience and thinking of the whole system as it lives and is used by users. Section 7 covers legal and governance issues.

2 Basic Organization of System

The basic organization of the system is simple. As in all software applications, there is the user interface with some front-end logic, there is a back-end business layer, and there is a database.

The main database of interest here is the blockchain. The patient health data is stored on the blockchain. A blockchain is not only a storage mechanism but there is code inherently associated with it for the proper handling of data and transactions. Whereas the blockchain acts as a record of the writes of health data, the logging of reads of the health data by various users and organizations is also important and is recorded on the blockchain. The blockchain is replicated across computers; each such computer is called a node. The blockchain is accessed by the server-side business layer and presented to the users via the user interface. There is a separate database for basic information such as users, their system passwords and access privileges.

In general, there is back-end interface for the input and output of data. There is an intake of data from external sources. In some cases, there is direct user entry of data via the user interface but in most cases, especially for historical data, the data is pulled in from external systems with permission. Bulk data desired by doctors or organizations such as research groups would be provided to them based on the permissions granted (Fig. 1).

3 Getting Started with Blockchain Development

3.1 Some Simple Use Cases

To understand how blockchain development is carried out, a set of simple scenarios can serve as a good start.

One blockchain was created for the referral of patients to specialists for the continuity of care. The patient health data was placed on the blockchain by the primary care doctor, and the specialist could then access the data and add to the health data as treatment progressed. A very similar blockchain was created for second opinion by expert doctors. The data would be segmented so that different experts could view the data of one patient and provide their opinion on the best treatment. Both these blockchain-based systems were created for customers in the USA.

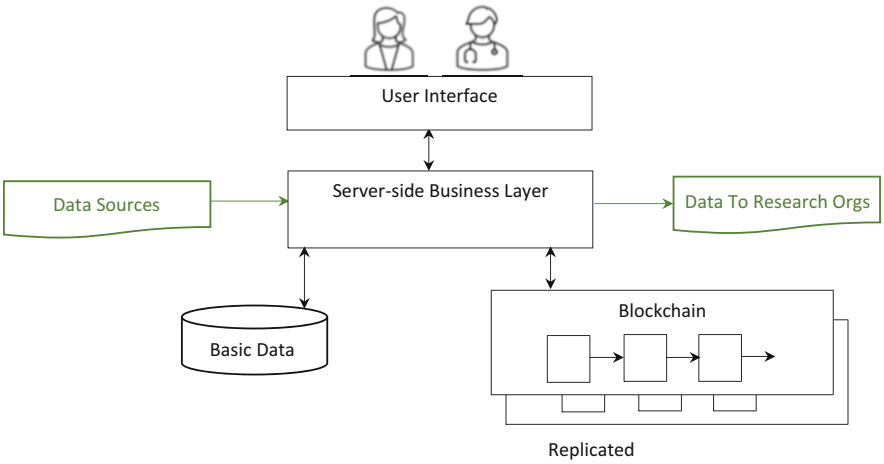


Fig. 1 Simple organization of Blockchain-based system

From these examples, the development process consisting of analysis of the problem, the solution design, and the implementation of the blockchain system can be studied.

3.1.1 Analysis: What Is to Be in Blockchain and What Is Outside the Blockchain

To proceed with the system, the main question to be asked is to what aspect is the blockchain applicable? In these two situations, the patient health history and current problems are of interest, so they are placed on the blockchain. The payment for services or insurance is not of critical importance, so that continues to be with the doctors' current systems. There is no need for data to be fed to research organizations, so they do not come into the picture.

3.1.2 Design: Define Roles and the Care Coordination Workflow

Now, the user roles and workflow are examined. The user roles are the Primary Doctor and the Expert Doctor. There can be sub-roles such as a doctor's assistant for doing some of the tasks. There is System Administration for the creation and exit of Primary Doctors and Experts. The main workflow is the addition of the health data—the historical and the current by the Primary Doctor, and the reading of that data and the addition to that data by the Expert (Ali, 2021). From an application viewpoint, the actions are View Health Data, Add Health Data, Assign Expert to Health Data (a set of related health records) plus some administrative actions such as View Primary Doctors, View Experts, Add Primary Doctors, View Usage Statistics, etc.

3.1.3 Implementation: Define the Detailed Parts—Blockchain and Business Logic

The next big activity is to map the software application world to some of the peculiarities of the blockchain world. This is a matter of terminology. The following are the main parts.

There is code for the blockchain to do its work. It is called smart contract, chaincode or similar. Essentially, it enables writes to the blockchain, reads from the blockchain, doing conditional coding (if-then) and looping. The basic unit of work is a transaction. So, the writing of one health data record is a transaction. As the recording of permissions is important, that is a transaction. The recording of who read what is important, so that is a transaction.

The identities that write and read are called as addresses. So, writes are done on behalf of a user, that is, one address. A read is done on behalf of the same user or another user, so those addresses come into play. Reads are done with the public part and writes are done with the private part of the public–private key pair that constitutes an address. The server-side back-end code needs to provide this to the blockchain as part of the transaction request.

All transactions can be read with appropriate permissions. In a general blockchain like Bitcoin, anyone can read the transactions between two entities, which is two addresses. That cannot work with private data such as health data. So, for reading a health data record, firstly the permission has to be read from the blockchain. It is possible that permission was given and then revoked. The latest permission setting is the one that comes into play.

The transactions and blockchain reads are submitted to the nodes of the blockchain. Depending on how nodes are laid out, the user entities may or may not have their own node. (See section "Copies of the Blockchain" below.) If a user entity has their own node, the server-side back-end code can submit the request to it. Otherwise, the server-side back-end logic needs to determine to which node a request should be submitted. This can be determined based on geographical nearness, the current load, or similar such considerations.

Some blockchain implementations utilize a fee for carrying out a transaction. In broad applications such as health records, such micro-fees for each transaction probably confuse the big picture of providing proper healthcare. But as the blockchain demands the fee, the server-side back-end code needs to provide it. This needs to be resolved at a higher level within the system—either by periodically topping up the fees for each user, or, accumulating and settling them over a period such as a month.

It can be seen from the above that there is blockchain code which does the job of storing, maintaining, and retrieving the blockchain data properly. There is server-side code that feeds the blockchain as needed and accepts the data that the blockchain provides. The server-side code connects to the user interface and to the external data sources and data sinks.

Separate from the blockchain data there is a need for a small database to keep track of the users who are the Primary Doctors and the Experts. The retrieval and update of current and historical users is done using this database. If users need

passwords in addition to public–private key pairs, then passwords are stored in this database.

For the segmentation of data for second opinion by Experts, the server-side business layer is slightly different. It needs to handle the splitting of data and possible determination of the appropriateness of the expert to whom the data is permitted (for example, renal data to a renal specialist verses an orthodontist). The blockchain code is unaware of such business layer considerations.

3.1.4 Summary of Development

The process for handling of the health records between the Primary Doctors and the Experts is, thus, the identification of what will be placed on the blockchain, the user roles, the workflows between the user roles, and the separation of what the server-side code does with the blockchain and what it does with the basic database. The blockchain code for managing the health application needs to be written to ensure the privacy of the health records, which is different from that of other blockchain applications. The server-side code interaction with the blockchain needs to be in accordance with the terminology and requirements of the blockchain (addresses, public key, private key, which node, etc.).

3.2 More Complicated Use Cases

One blockchain application was created for the utilization of patients' health data for clinical trials. Clinical Research Organizations reach out to patients for their data and offer payment for the data. With the data being on the blockchain, patients can provide access to the organizations to the parts of the historical data or current data as per mutual agreement. For the ease of use by patients, this included a mobile phone front-end for popular phone operating systems. This was for a US-based customer.

In addition, two different blockchain applications were created for the aggregation of health data for research into diseases. The research organizations pay the patients for access to their health data in a manner like clinical trials as in the above paragraph. One of the applications was for a US-based company whereas the other was for a Europe-based organization.

3.2.1 The Development Process and Sub-Parts

The development process is the same as indicated in the previous section.

What part needs to be on the blockchain? The health data, for it to be trusted by the entities involved. The payment information, for the purposes of completeness, traceability, and trust. Going "upstream" from the payments because payments depend on the permissions given to the various organizations for the access to the pieces of the health data, the permissions should be on the blockchain.

The number of entities is much larger. To keep it simple, the user roles are Patient, Doctor, and Buyer, where Buyer is the organization requesting the data for either clinical trials or disease research.

3.2.2 The Workflows

The workflows are sightly complicated. In addition to the write of the health record, the read permissions and the payment need to be handled.

The following gives a glimpse into the permission workflow. The permission can be provided by the patient to one Buyer on a per-record basis, or it can be to one Buyer on a blanket basis, or it can be to a slate of Buyers on a blanket basis. If permission is not already provided, then a Buyer may request permission from a Patient; again, this can be on a per-record basis or a blanket basis. The time aspect needs to be considered; requests for permission could be ignored, reminded in a timely manner, or, could time out. All permissions need to reside on the blockchain (Waghmare, 2020).

For payments, the following is a glimpse into the workflow. When a request is made to read a health record, the permission is checked. If permission is provided, the health record is read from the blockchain, the read event is recorded, the payment is computed and recorded on the blockchain, and notifications are sent to the Patient and the Buyer.

The blockchain code is written with all the above requirements. That development is similar to the one already described in the previous section. The complexity introduces issues to be considered; these are given in the sections below.

3.2.3 Business Logic and User Interface

As is to be expected, the server-side code is significantly more complicated. It includes all the aspects of client–server system creation. This covers the handling of incoming bulk data and outgoing bulk data too. One aspect that could be unique is interfacing with crypto exchanges if cryptocurrency is utilized (but also see section "The cryptocurrency aspect" below). The blockchain connection likely throw up issues; these are given in the sections below.

The user interface needs to sensitize the users about possible transaction times (see section "Speed of the Blockchain" below). The user profile also needs to be considered. Whereas mobile phone applications are common now, if the user interface is mobile phone, then users may need some training and guidance on how and why things are different when a blockchain is involved.

3.3 Stepping into Detailed Considerations

The different aspects to be considered for actual implementation of such a system and taking it into sustained and successful production are given below. The aspects are organized from a low-level to a high-level.

Getting all the health record data is a complicated topic in itself. As it is not exclusively related to the blockchain technology, it is not covered here.

4 Organization of the Blockchain

4.1 What Is on the Blockchain and What Is Kept Separate?

Whereas some health records are small in size, some files such as radiology images can be huge. They are typically 5–16 MB but can be as big as 50 MB (Ohal, 2021; Seibert, n.d.). Blockchain blocks are typically limited in size; the block size is based on considerations such as the rate of arriving transactions, and the computation and coordination needed to create the blocks. Typical block sizes are 1 to 8 KB. Because of this, voluminous files need to be stored separately. They are stored in an encrypted manner in global, replicated databases such as IPFS or Cosmos DB. The hash of the data in the file, the date of creation, the file identifier, and other key characteristics are stored in the blockchain (Fig. 2).

4.2 Small Health Records Can Be Large for the Blockchain

Some health records may simply be larger than one block or a few blocks. A single, non-image medical record can be 4 to 60 KB in size. Typical block sizes are 1 to 8 KB. One technique to manage this is to increase the block size if this can be accommodated along with the rate of arriving transactions, and the coordination needed to create blocks.

That may not suffice for most health records. Health records need to be split so that they span multiple blocks. Typical health records have multiple sections such as identifying demographics, medications, problems, etc. One way to split would be by sections, as given in the figure below (Fig. 3).

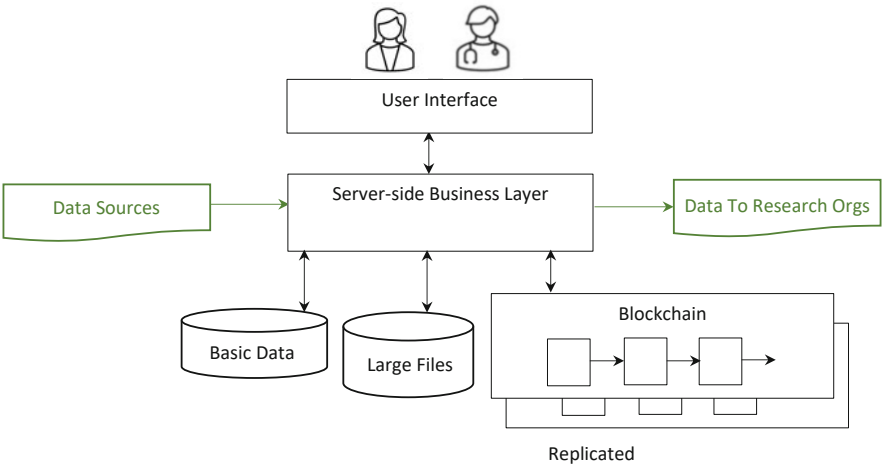


Fig. 2 Blockchain system with large files on global database

Fig. 3 Splitting a health record

Another way of splitting would be to simply chop the record into pieces that each are just under the block size and add some identifying information to each part (Sharma, 2017).

The parts need to be re-assembled into the complete health records during a read. The server-side back-end logic needs to do the splitting and re-assembly. Also, see "redacting" in section "Compliance as per country and state" below.

4.3 How Many Copies of the Blockchain?

The thinking among the entrepreneurs and visionaries often is that as they add partner organizations such as research groups or non-profit organizations to be part of the ecosystem, each of those can maintain a copy of the blockchain. Given the prevalence of cloud systems in today's world there is no need for such one-to-one equivalence between partner organizations and the copies of the blockchain.

However, when the system is spun up, there may not be any partner organizations or there may be just one or two. For the authenticity of the blockchain, the blockchain should have at least five copies.

Moreover, if the number of users and the number of records are small in the initial ramp up phase, then for the sake of the trust and confidence in the blockchain, the number of copies should be larger. Nine or more copies would generate sufficient confidence in the user and partner community.

These copies are best distributed as widely as possible geographically. Whereas countries have restrictions that data should not cross the boundaries (see section "Compliance as per country and state" below), the distribution should be as spaced out as possible within a country.

4.4 How About Blockchain on Mobile Phone?

Given that people use their mobile phones a lot there are attempts to put copies of a blockchain on phones. This may work for some types of records and data. However, a blockchain does not simply have one individual's data. Each block of a blockchain has data from several users. All that data is tightly bound with the hash of that block. Given that health records will be for many users, that each user's health data spans many decades and also given that some records will be large, keeping health data blockchain copies on a phone is impractical.

To get a feel for the volume, a rough computation can be carried out. A single, non-image medical record can be 4 to 60 KB in size. A patient generates close to 80 MB of health data per year including imaging data. Keeping the image data off the blockchain with only the key information on the blockchain perhaps reduces each patient's yearly data on the blockchain to about 0.5 MB. Whereas a patient's lifetime is fairly long, let us assume that medical records are for a period of 20 years. So, that makes a single patient's data to be 10 MB. For 100,000 patients, which is a fairly small subset of any population (by location, by community, by disease, etc.), this amounts to 1 TB of data.

Thus, for other than a few, niche, health record blockchain applications, keeping blockchain copies on a mobile phone is infeasible.

4.5 Proper Handling of Bulk Data

The ability of the blockchain to handle bulk data input needs to be tested beforehand, and if needed, strategies for handling bulk input need to be planned.

The situation may arise when users upload their historical health data records. If the records are split and submitted to different nodes in a concurrent manner, then the different nodes may decide to prioritize separate sets of records, that is, blockchain transactions. Normally, the consensus mechanism will ensure fairness and handle the transactions in a timely manner, that is, process first-in-first-out in an overall sense (though not in an exact sense for every transaction request). However, if the load is too even, the blockchain may create ommer blocks (uncle blocks) and then spend significant time trying to resolve those, leading to incoming transactions piling up.

Another situation is when sustained bulk load is applied as input, then the blockchain performance falls off and can take a few minutes to recover.

If this situation is possible and is identified during performance testing, then strategies of load balancing, introducing gaps in the load or higher-level prioritization may be needed in the business layer to ensure that all health records are handled in a timely manner.

Another possible solution that may work in some situations is to use elevated CPU or GPU processing power. This can be a temporary solution for a few days if a backlog of health records is to be processed. This has significant cost implication and is not a long-term solution (Kulkarni, 2019a). This will work only if there is control

over all the nodes of the blockchain but not if the nodes are distributed across parties (see section "How many copies of the blockchain").

5 Selection of the Blockchain Technology

The basic concepts of the underlying blockchain technology are fairly clear—gather transactions, have the nodes create consensus regarding which transactions are to be placed into a block, create the block including its cryptographic hash, share this block with the other nodes so that every node then connects the block to the previous block and thus maintains the chain. Should you then create your own blockchain technology or select one of the available ones?

5.1 Speed of the Blockchain and Record Retrieval

The time that a blockchain takes to generate one block can be an important consideration. Because multiple transactions are assembled and put together, and different nodes of the blockchain could assemble different sets of transactions, they need to come to consensus about which transactions to assemble. This implies that any single transaction takes a much longer time to be completed/committed compared to the currently prevalent centralized transaction processing systems. Typical blockchains take 1 second to 20 seconds to assemble a block. Some transactions will "miss" the current block and will have to be taken up for a subsequent block. This needs to be factored when uploading bulk data as well as when an individual user is submitting data (Patel, 2020). And also, when a user does meta-level actions such as giving permission to an organization for accessing the data—because such transactions are also on the blockchain.

Retrieval of data needs to go backwards through the blockchain assembling records as they are found. Older records take longer to be retrieved (Joshi, 2020).

As the blockchain gets longer, its response time slows down. This is for writes as well as reads.

All these aspects must be considered as part of the system characteristics as well as from a user experience viewpoint.

5.2 Widely Used Blockchain Technology or a Professional-Seeming One?

The intrinsic blockchain technology needs to be very carefully engineered. It is easy to have holes and gaps in the technology which may manifest—suddenly and severely—in security and performance. Malicious actors try to exploit defects and new aspects are discovered every year. As a result, creating your own blockchain technology is a highly challenging activity. You must rely on existing blockchain technology created by other organizations. Ethereum (ethereum.org) and

Hyperledger (Hyperledger.org) are among the well regarded multipurpose blockchain technologies.

The technology needs to be open source so that multiple people around the world have already examined the code, pointed out flaws, and the code has been updated to repair those flaws. Some blockchain technologies keep most of the code open while withholding some code. Trusting such technology could turn out to be highly problematic and is best avoided.

Both Ethereum and Hyperledger have been used for the example customer systems described in the above sections. Ethereum has the ability to plug in different consensus algorithms. Hyperledger has two strong implementations in Fabric and Sawtooth. Sawtooth is more flexible than Fabric (Anwar, 2021). Sawtooth supports Byzantine Fault Tolerance, four consensus algorithms including Proof of Elapsed Time (POET), and supports the coding languages Rust, JavaScript, Go, and Python.

5.3 The Cryptocurrency Aspect

Blockchains can use tokens for transactions, that is, accept payments in the form of tokens for record updates and for record retrievals. It is tempting to float a new cryptocurrency which will gain value as the blockchain adoption increases over the years. However, any currency must deal with multiple aspects of economics such as speculation, inflation, convertibility with other currencies, attacks on the currency, and so on. If the main aim of the blockchain is to handle the health records for the benefit of patients and the medical community, then it is best not to embark on the cryptocurrency path and simply use ordinary, fiat currency.

6 Thinking of the Complete System

6.1 Secure Access to the System

Whereas the data on the blockchain is secured by the nature of the blockchain, all access points to the system should be secure too. This includes the databases, the portal, and all interfaces.

Malicious agents will try to exploit the system for financial gain as health data is quite valuable. Rather than grabbing the data from the blockchain directly, they would simulate the actions of legitimate users. They would attack the basic database of logins or the user interface and exploit vulnerabilities there. By acting like legitimate users, they may siphon off the data.

Other reasons for malicious attacks include revenge, sabotage, vandalism, corporate espionage, or quite simply the challenge involved. A very basic attack could be a Denial-of-Service attack by which unrelated requests flood the system leaving genuine users unable to access services (Cloudflare, n.d.; Fortinet, n.d.). To prevent all such attacks, not only should the application security should be verified by penetration testing but also the system should be secured with complete website

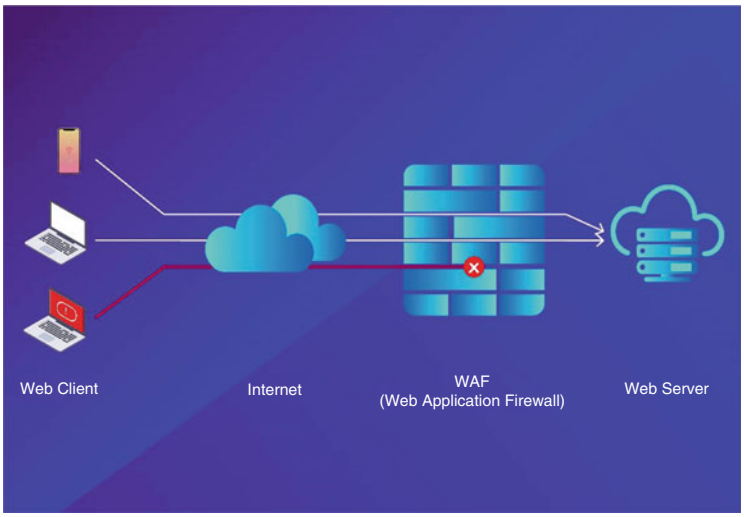


Fig. 4 Website security software

security software (Shekhawat, n.d.). This is shown in the figure below, where the security software handles legitimate access and bars suspicious access (Fig. 4).

6.2 The User Experience Matters

The main reasons for a blockchain-based system of health records are the trust and sharing of records. Whereas that is a necessary basis for the system, the whole system should be designed properly for the users and partner groups. Performance and reliability are important. The user interface should be pleasing and easy to use. There should be notifications and warnings as appropriate. There should be proper online help as well as error messages. The handling of bulk data imports and exports should be proper with adequate messages and with retries as needed.

For all the customer systems mentioned in the above sections, the user interface was tried to be kept as close to the current world-class application systems as possible. This was irrespective of a web front-end (Kulkarni, 2019b) or a mobile phone front-end (Sharma, 2018).

If users get turned off by any part of the system or its performance, they are likely to stop using the system. After that recovering from such losses and getting other users on to the system is an uphill battle.

The user experience matters a lot.

6.3 User Sensitization and Training

Some aspects related to the intrinsic blockchain need to be introduced, explained, and reinforced to the users.

Because a blockchain transaction can take time, the users need to have asynchronous submission of records and requests. The users submit first and can then do other, unrelated actions within the system. When the health record is committed by the blockchain in its entirety (possibly over multiple blocks, as in section "Small health records can be large for the blockchain" above) or a health record is read, then a notification can alert users so that they can choose to take the next step. This delay is not intuitive and users may not understand the underlying cause, so it needs to be explained when they start off (Waghmare, 2018).

Users need to be told clearly and often that their private–public key pair is unique to them, and it must not be lost. Whereas there are some ways to seed keys, most systems do not do this at the outset.

If cryptocurrency is involved, then users may need to be told about the risks in cryptocurrency (see section "The cryptocurrency aspect" above).

In general, users are not blockchain enthusiasts; they are doctors, patients, researchers, and so on. Hence, detailed aspects such as the tracking of transaction queues, the completion of transactions, the transaction fees, a node going down and so on by viewing the details of the blockchain activity need to be handled carefully. Either this should be kept hidden from all users (by allowing actions such as View Health Data, Add Health Data, Assign Expert to Health Data as in section "Getting Started with Blockchain Development" above) or only self-professed, advanced users may be allowed to view these aspects.

6.4 Responding Quickly to User Issues

When a system is in production then issues like down time and software quality come to the fore.

Keeping the system working properly as per Service Level Agreements promised to the users is extremely important. Down time for upgrades must be carefully coordinated across nodes and must be kept minimal. Blockchains are built such that one or more nodes may go down; when nodes come up, they copy the blocks already created and catch up. However, excessive down time for any node can become problematic.

All systems have defects. Even if testing is fairly robust, users may use the system in ways that are unexpected and unplanned. When issues crop up, they need to be handled quickly. A system may have good intentions and may draw in users in a fantastic manner, but users should not be lost due to bad service or unsatisfactory user experience.

7 Compliance and Governance

7.1 Compliance as per Country and State

Compliance with the laws of the countries in which a system operates seems to be too obvious to even be stated.

If your system spans multiple countries, you may want a separate instance of the blockchain for the users and organizations in each distinct country. That would need to be coupled with country-specific configuration of the system, possibly along with the business layer using country-specific rule engines.

Whereas raw data may not be transferable across country borders, aggregate data and insights can possibly be shared and sold. Thus, there would need to be a distinction between the type of data access that is provided, and the users need to be properly told and continuously guided on the distinction.

Even within a country, different states may have different laws. For example, the USA has HIPAA (Health Insurance Portability and Accountability Act) as the main law regulating health data. However, the states of California, Colorado, Connecticut, Utah, and Virginia have comprehensive laws related to consumer data privacy (NCSL, 2022). Some states may emphasize SOC (System and Organization Controls), especially SOC2, related to trusted services.

GDPR (General Data Protection Regulation) and related laws indicate that a user may choose to have some of their data deleted. Whereas it is not possible to simply delete old data out of the blockchain (as that would affect the hash of that block and all the subsequent blocks of data), a "redact" mask would have to be applied to that data. Thus, if a patient had a health record in 2020 that was requested to be "deleted" in 2022, then every read access by anyone after that request would need to retrieve the redact information first and mask out that specific health record of 2020.

7.2 Audit Access to the Blockchain

For building trust in the blockchain, audit access must be built into the blockchain. The auditors would be agencies other than the user community and the partner community. They could be governmental agencies or professional third-party audit companies.

The actual data that is added and shared must not be shown to the auditors. The data seen by the auditors would be the high-level data stored on the blockchain such as the date-time of data reads, and, whether the data reads correspond to the permissions granted to the reading user/organization. The "if and only if" constraint on the data sharing should be viewable by the auditors (Fig. 5).

The figure shows the blockchain on the left. The blockchain has health records as well as permissions given to other users. An audit, as shown on the right, examines some or all the permissions.

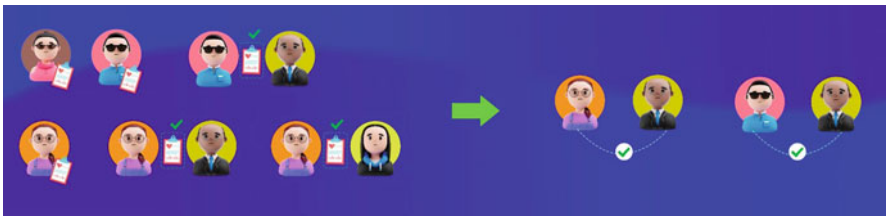


Fig. 5 Auditability of the Blockchain

This auditability is a fundamental characteristic of a system for something as crucial and regulated as health records. It needs to be built-in at the start. It cannot be retrofitted on the system.

7.3 Governance

For further building trust in the system a governance structure is important. Whereas the governance structure may not be present when the system is originally conceived and created, it is important for guiding the changes that need to be made to accommodate evolving types of users or the evolving needs of different stakeholders.

The governance could be through a body of directors, with the inclusion of some independent directors. This is the business norm for for-profit companies as well as non-profit organizations. This can be utilized for the blockchain-based system too.

In accordance with this, one of the customers has a governance structure wherein independent non-profit patient associations are a part of the body of directors, along with people from reputed, international pharmaceutical companies.

For blockchain governance, instead of a body of directors, there could possibly be a decentralized autonomous organization, or DAO (Weston & Beginner's Guide To Decentralized Autonomous Organization Or DAO, 2021). The basic concept is that the voting power is decentralized among all or a large number of stakeholders. At this time, there are different types of DAOs and the goodness of the DAO concept is not clearly established across businesses.

8 Future Directions

As blockchain-based systems for patient records get created and released for usage by patients, doctors, researchers, and the public further issues of efficiency and usability will get discovered. They will require immediate engineering solutions in order to satisfy the users. They will also force the development of engineering solutions that will prove robust for the next few years. Concepts in blockchain such as consensus algorithms and efficient storage will continue to evolve. This

indicates that those involved in designing and implementing blockchain-based system need to keep abreast of the latest developments.

9 Conclusions

The main motivation for creating a blockchain-based system is to utilize the advantages of blockchain technology. That is straightforward. For a successful implementation of the system, the aspects mentioned here need to be kept in mind, addressed, and planned for. Whereas the focus here is on how the characteristics of health records impact the usage and the success of the system, some of the aspects have general applicability and would need to be considered for blockchain-based system that aim to provide solutions in other domains and verticals.

References

Peral, J., Gallego, E., Gil, D., Tanniru, M., & Khambekar, P. (2020). Using visualization to build transparency in a healthcare blockchain application. *Sustainability, 12*(17), 6768. https://www.mdpi.com/2071-1050/12/17/6768

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings–2016 2nd international conference on open and big data, OBD*. https://doi.org/10.1109/OBD.2016.11

Ali, T. (2021). *Harbinger systems private correspondence on organization and data interface*.

Waghmare, S. (2020). *Harbinger systems private correspondence on permission workflow*.

Ohal, P. (2021). *Harbinger systems private correspondence on sizes of radiology images*.

Seibert, J. A. (n.d.). *Archiving: Fundamentals of storage technology, chapter 2: Medical image data characteristics*. SIIM, University of California, Davis. https://siim.org/page/archiving_chapter2

Sharma, M. (2017). *Harbinger systems private correspondence on data record splitting*.

Kulkarni, R. (2019a). *Harbinger systems private correspondence on CPU-GPU cost*.

Patel, N. (2020). *Harbinger systems private correspondence on performance*.

Joshi, S. (2020). *Harbinger systems private correspondence on performance*.

Anwar, H. (2021). *Hyperledger Sawtooth Vs. Fabric: How are they different?*. https://101blockchains.com/hyperledger-sawtooth-vs-fabric/

Cloudflare. (n.d.). *What is a DDoS attack?* https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Fortinet. (n.d.). *What is the difference between DoS attacks and DDoS Attacks?* https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos

Shekhawat, V. S.. (n.d.). *What is a DDoS attack and how to mitigate it*. https://www.loginradius.com/blog/engineering/how-to-mitigate-ddos-attack/

Kulkarni, R. (2019b). *Harbinger systems private correspondence on user experience*.

Sharma, M. (2018). *Harbinger systems private correspondence on user experience*.

Waghmare, S. (2018). *Harbinger systems private correspondence on user sensitization and training about the blockchain experience*.

NCSL. (2022). *State Laws related to digital privacy (originally, state Laws related to internet privacy)*. https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy

Weston, G. (2021). *Beginner's Guide To Decentralized Autonomous Organization Or DAO*. https://101blockchains.com/decentralized-autonomous-organization-dao/

Prashant Khambekar has worked extensively in commercial software, after obtaining a Computer Science doctorate in distributed computing. The work encompasses engineering, process, and business and touches wide-ranging domains such as supply chain, healthcare, and human resources. Prashant Khambekar has spearheaded innovation in Internet of Things, Data Science, and blockchain. The work in healthcare software spans several years and includes claims processing, Internet of Things for healthcare, patientcare software, pharmacy software, clinical trials, telehealth, etc. The interest in applying blockchain in healthcare goes beyond patient records to billing, claims and systems for nurses.

Blockchain Implementation for Decentralized Real-World Research

Rhea Mehta, Francisco Diaz-Mitoma, and Cesar Diaz

Abstract

The goal of this chapter is to demonstrate that a patient centric and data-driven approach are required to develop blockchain-based health applications that are useful for patients and healthcare providers. Bowhead Health, describes a case study of such an application to identify people with migraines that required a community-building educational approach. We first describe how a private, Ethereum blockchain platform within the pharmaceutical and consumer health sectors was implemented, including its objectives, key features, adaptations, and implementation steps. Next, we discuss our key learnings and the challenges faced in implementing the blockchain health data case study. In particular, we explore the importance of the community building and education approach that was used as an adjunct tool to support the mindset shifts necessary for blockchain applications to have a beneficial impact in healthcare.

1 Introduction: Data Ownership and Management in Healthcare

The size and value of health data are growing and are expected to reach $34.27 billion by 2022 with a compound annual growth rate of 22%. It is therefore no surprise that data science is growing faster in healthcare than in any other industry given the breakthroughs, savings, and advancements possible with big data analysis (Lucassen et al., 2021).

As the health data economy continues to flourish, a critical question of ownership is raised by several patient-centered stakeholders in the industry. Concerns around

R. Mehta (✉) · F. Diaz-Mitoma · C. Diaz
Bowhead Health, Kanata, ON, Canada
e-mail: drrhea@bowheadhealth.com; fdmjr@bowheadhealth.com; cesar@bowheadhealth.com

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_8

ownership are validated by the historic mismanagement and misuse of health data by large organizations, institutions, and third-party companies, including:

- The monetization of data without appropriate disclosures
- Data leakages and ransomware cyberattacks due to IT vulnerabilities
- Granting access to data for AI model training/analysis without consent
- Mistakenly releasing patient records containing personally identifiable information

A notable example is the 2020 cyberattack of Canadian medical testing company LifeLabs that exposed the sensitive personal information of an estimated 15 million Canadians. The LifeLabs data breach included test results and health card numbers along with personally identifiable information including names, dates of birth, home addresses, and email addresses. Login IDs and passwords may have also been compromised in the breach. Lawsuits claim that the breach was related to inadequate cybersecurity controls and safety protocols and that the stolen data was stored unencrypted on non-secure servers, with poorly trained staff managing the data (Ikeda, 2020).

While the emergence of big data in healthcare has resulted in enormous opportunities for the industry and patients, it also raises important ethical and legal questions around patient data privacy, security, management, and control that especially need to be addressed in this new era of digital health monitoring and data collection (Kerekovska et al., 2020; Agrawal & Prabakaran, 2020; Wu et al., 2022).

In this chapter, we describe a use case for which we implemented blockchain technology within the pharmaceutical and consumer health sectors to protect patient data from leakages and mismanagement and shift the ownership and power back to patients. We first discuss the value of blockchain in healthcare and the concept of real-world evidence and its importance for the pharmaceutical industry, then reveal the design and key features of the blockchain solution we implemented, as well as the winding process by which the solution was implemented. We end the chapter by presenting our learnings and illuminating the importance of a community-building approach in implementing disruptive innovations such as blockchain.

2 The Value of Blockchain Technology in Healthcare

Blockchain is defined as a type of distributed, digital ledger technology that consists of a growing number of transactions, referred to as blocks, that are securely linked together through an encryption process known as cryptography. Each block is bound to the previous block through a cryptographic hash and a timestamp is logged with each block to validate that the data associated with the transaction existed when the block was created. Each block contains information about the block previous to it, which effectively forms a chain, making it impossible to alter a transaction without having to alter all blocks in the chain. Any attempt to change records will be immediately recognizable and notify the validators of the blockchain (Wikipedia, 2022).

Because it is distributed across several computer systems, one centralized authority, such as a hospital or government cannot be in control of the data. Instead, the data is controlled by the patient, or whomever the patient has decided to give control to. All terms and conditions for each transaction are recorded into a digital contract, known as a smart contract, which is computer code that self-executes according to the terms laid out in the agreement. In this way, no intermediary is necessary to manage the collection, transfer, and storage of the data. Furthermore, because each transaction is encrypted, the data cannot be linked to any personal identity.

The technology is therefore considered decentralized, as well as secure, self-sovereign, anonymous, and transparent. Using blockchain technology, patient data, including lab tests, consultation history, clinical trials, and research information, and patient consent data are more reliably stored and better managed, with fewer risks of misuse.

3 Real-World Data Collection in the Pharmaceutical Industry

Real-world evidence (RWE) in pharmaceutical drug development analyzes real-world data (RWD), such as medical records, data from wearables, and other digital health tools like surveys to learn about symptoms and medication history. Pharmaceutical companies use RWE to complement data from clinical trials and learn more about the safety and effectiveness of their drug in a patient's daily life. The US Food and Drug Administration (FDA) defines RWE as "the clinical evidence regarding the usage and potential benefits or risks of a medical product derived from analysis of RWD."

While RWE helps researchers understand how patient disease and drug experiences affect health outcomes, key challenges need to be addressed as the use of RWE continues to expand. These include improving data collection, data quality, and data security, capturing patient consent, preventing personally identifiable information from being collected, and improving the means of analyzing relevant data to mitigate possible biases (Roussanov & Mulryne, 2021). Incentives or financial rewards could also be considered to reward data contributions by patients, given the evidence that providing financial rewards can boost medical adherence. Using blockchain-based incentive approaches would allow users to remain anonymous while receiving payment.

Addressing these challenges will be important to ensure the value of any RWE collected, as well as ethical considerations as it relates to patients, and ultimately, the success of any product that seeks to rely on it.

4 The Bowhead Health Case Study

In this section, we introduce the case study of Bowhead Health. We begin by describing its business and the properties of its blockchain-based, real-world evidence-capturing platform.

Founded in 2015, Bowhead Health (BHH) is a Canadian company aiming to democratize healthcare. BHH builds software solutions that leverage encryption, blockchain, and smart contract technology to help individuals safely own and share their health data. BHH believes that creating tools for secure data ownership is essential for us to realize the potential of data-driven healthcare and can truly revolutionize how we deliver patient-centered care.

The key product of Bowhead Health is the BHH platform. BHH is a General Data Protection Regulation (GDPR), CE Mark Class IIa, Health Insurance Portability and Accountability Act (HIPAA), Health Canada, SOC 2, ISO 27001, and NIST-compliant data management platform. Data residency is built into the platform, meaning Bowhead can keep the data localized on specific regional servers, which is in line with regulatory requirements. The Better by Bowhead application also underwent a digital review in 2021 by The Organization for the Review of Health and Care Apps (ORCHA).

The BHH software platform enables researchers to launch end-to-end encrypted RWD capturing programs on the Better by Bowhead mobile application that encompasses:

- Diverse patient recruitment
- Custom symptom or disease-specific questionnaires
- Daily health behavior tracking
- Secure data storage
- Transparent eConsent capture for anonymized data sharing
- Smart contracts that ensure patient data-sharing incentives
- Distillation of health data insights on a Research Dashboard

Traditional health data platforms for conducting patient research follow a centralized architecture approach. Centralized architecture creates inherent security and privacy risks. Failing to provide patients with true ownership and control of their health data also exposes life science organizations to unforeseen risks. As shown in Fig. 1, traditional health data platforms rely on third-party software owners to verify and transmit data when data access is requested, which creates an inherent risk of data leakage or invasion of privacy as there are administrative staff involved in the process and little technical infrastructure to shield risks. In contrast, our solution begins with data owners giving consent to data sharing, uses smart contracts to fend off any human interferences, and ensures that data can only be accessed in a de-identified manner, minimizing security and privacy risks while simplifying the data-sharing process.

As shown in Fig. 2 below, the BHH platform consists of several layers that work together to create a flexible solution, with blockchain being the central part of the system. From there we added an immutable and private layer to handle user consent, managed by smart contracts. The platform was built on the blockchain with the most developers, Ethereum.

Data Layer A major innovation introduced by Bowhead lies in our data security architecture. User data is encrypted with a powerful AES-256 algorithm, for which

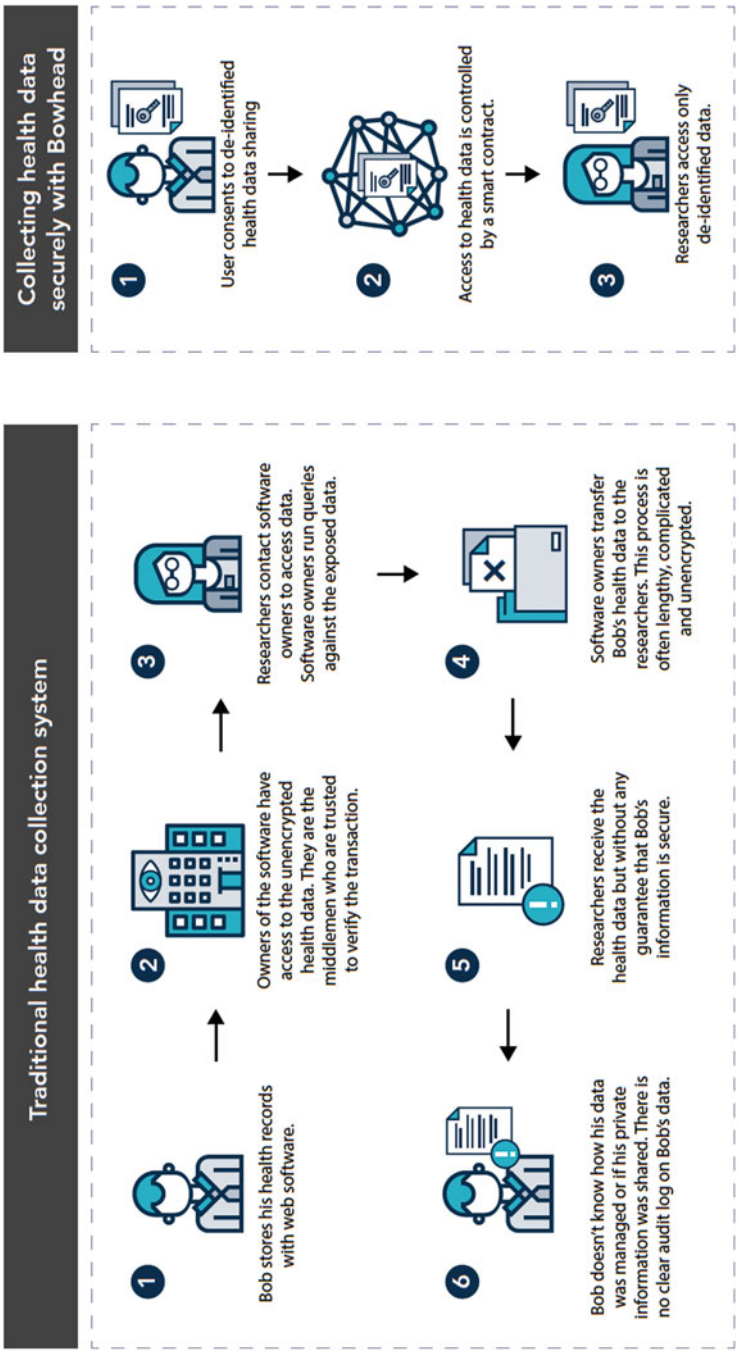


Fig. 1 Traditional health data collection vs. BHH platform

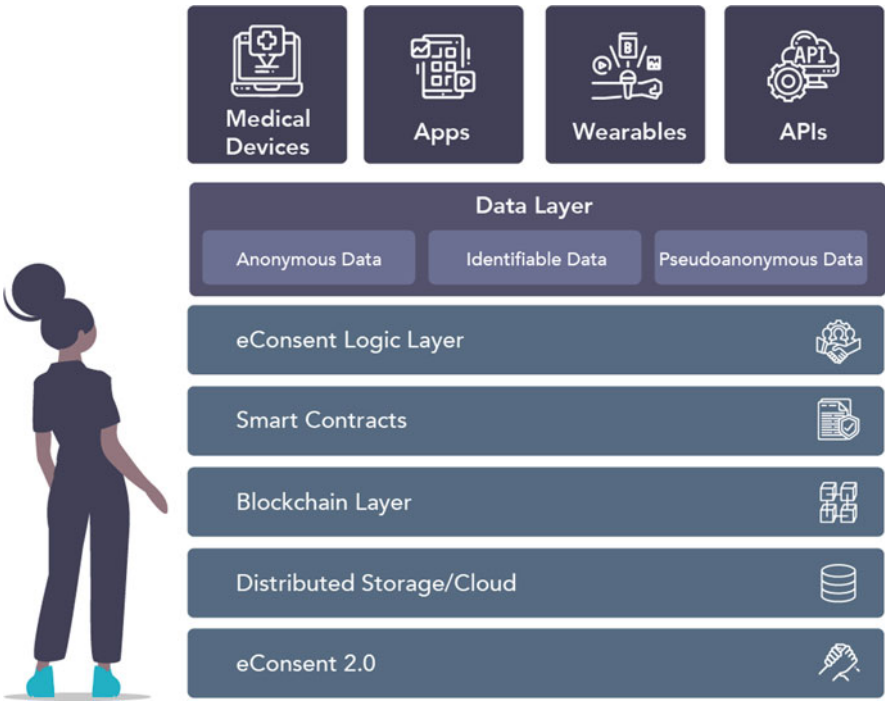


Fig. 2 Bowhead Platform Layers

only the user possesses a private key. During the onboarding process, users gain an understanding of the importance of data privacy and are guided to follow simple procedures to keep their data safe, which includes removing the need for email and phone number-based accounts. Bowhead's system architects, developers, and designers also worked alongside our collaborator's researchers to prototype and implement a novel data insights dashboard with built-in visualization features. The result was an end-to-end solution with data insights and near real-time analysis. Besides, BHH nor any other party has access to patients' identifiable private information. In regulated reporting, such as in drug safety or pharmacovigilance, in which BHH has also participated, Adverse Events must be reported with individually identifiable information. However, in this case, only the defined party receives an Adverse Event report using end-to-end encryption.

Smart Contracts and Blockchain Layer Bowhead Health's technology is designed for the patient's full privacy and empowerment by developing a platform using open-source tools provided by Ethereum's smart contracts. The safety of encryption keys through this technology gives health data ownership rights back to the patient, allowing them to decide how and when to share their data. These "keys" create a distributed ledger, which provides data immutability and secure portability. As aforementioned, smart contracts are autonomous pieces of software that ensure a set of rules are enforced and executed securely and transparently.

Through smart contracts, users are presented with an informed choice to share their anonymous data to benefit real-world research. Only once consent is granted is that user data stored in a de-identified manner on Bowhead's GDPR and HIPAA-compliant platform.

Distributed Storage/Cloud Layer The blockchain, with all its benefits, does have limitations. The data stored is not structured in a way that it can be analyzed efficiently. As a result, we added a distributed database layer that helps us use battle-tested tools to expose the analytics needed by the researchers to measure study outcomes. Using this mechanism, we can build dashboards to show any desired metric using anonymous aggregated data. In addition, BHH leverages both Amazon Web Services and Microsoft Azure services for maximum global hosting coverage. MongoDB is used when a database is required, for example, in the case of the data insights dashboard.

eConsent Logic and eConsent2.0 Layer BHH uses an Open Source Headless Content Management System which enables content to be dynamically modified using a RESTful API via an Administrator Dashboard. This ensures that patients have the right to withdraw from the study without intervention from Bowhead or another intermediary and each action taken by the patient is registered as evidence and cannot be altered in any way possible.

5 From Pilot to Global Digital Remote Patient Monitoring Solution

The implementation of the BHH platform began with a pilot. In 2018, a top 10 global pharmaceutical manufacturing company saw an opportunity to innovate in this area and collaborate with BHH to design a privacy-first RWE pilot program for people suffering from chronic migraines. Specific objectives included (1) optimizing how our collaborator collected data for research, with a focus on security, transparency, and privacy, and (2) gaining real-world evidence on migraine symptoms, triggers, and reliefs from a diverse and global audience. We envisioned the success of the pilot driven by three key differentiators: data protection, user consent, and ease of use.

Data Protection Patients have ownership of their data via private encryption keys and manage their private keys and transactions using smart contracts on a distributed ledger.

User Consent Patients control data sharing by clearly consenting to its use for research, and hold the power to cancel sharing at any time.

Ease of Use The Better by Bowhead mobile application is intuitive and user-friendly, making it easier to participate in a digital campaign on a serious topic.

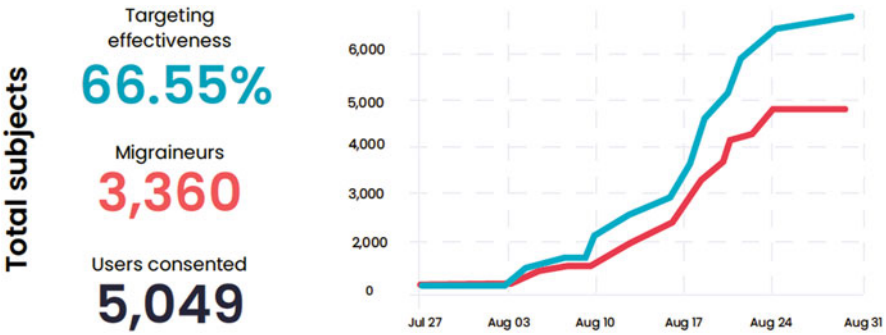


Fig. 3 Results of platform usage by 2020

Guided by these principles, we launched the pilot in July 2019 where we delivered an end-to-end solution for recruiting, capturing, and distilling unique insights on migraine sufferers. Within 3 months, Bowhead was able to recruit 1000 subjects from Germany, Switzerland, and Austria to consensually share their anonymous migraine data for research. Recruitment was accomplished either by patients' physicians or through targeted social media advertisements on Facebook, for example.

Following the success of the pilot in the three countries, the program was rolled out in 6 more countries in July 2020, including patients from Switzerland, Germany, Austria, Italy, Spain, United Arab Emirates, Denmark, South Korea, and Japan. By the end of 2020, over 6000 subjects successfully signed up as shown in Fig. 3, completed the migraine survey to report on migraine symptoms, and employed the application on their mobile phones to track symptoms and other health behaviors. This means that the BHH RWD program had scaled to 9 countries and moved beyond a simple RWD study to support patients along their journey to better health. What started as a migraine tracker on the Better by Bowhead application around patient pain points expanded to include healthy habit tracking. Data collected would then be used to connect interested study participants with migraine specialists in their local communities to seek guidance and support, with the ultimate goal of leading to better health outcomes. Patients would use the application to complete health questionnaires (i.e., logging their migraine symptoms and episodes) as well as track key health indicators (sleep, hydration, stool, energy levels, etc.). The application would also help them adhere to their treatment schedule via reminders and notifications, and monitor compliance via machine vision or audio-video detection to track pill intake. Once health data was consensually shared on the application, patients could continue to use the application to track and manage healthy behaviors and adhere to treatment.

The program also focused on educating patients on the merits of a privacy-first platform. We helped study participants learn about safe health data collection and sharing practices that are in the best interest of the patient. Research shows that when patients are transparently informed about the intentions behind data collection, they are very willing to share symptom data with scientists to advance medical research.

Based on data from our pilot, 30% of people were willing to consent to share their de-identified health data for research.

To add further strength and validation to our platform, Bowhead's approach was granted Unconditional Ethics Approval and third-party validation by the Veritas Independent Ethics Review Board (IRB). Veritas IRB is the oldest Canadian independent ethics review board constituted and operated according to the World Health Organization Operational Guidelines for Ethics Committees that review biomedical research. In a nutshell, all the data flow, collection, consent, and handling of the data were submitted to Veritas for approval.

In 2021, our collaboration moved beyond migraines to include an atopic dermatitis RWD study. This study was launched in Germany and Japan, Italy, and Spain and included several of the same features as the migraine RWD study, including symptom logging, healthy habits tracking, and consultation with local dermatologists. Patients were also empowered to log symptoms off-screen, and seamlessly import them by taking a photo post-episode of their skin conditions.

By the end of 2021, we recruited over 10,000 subjects and expanded to another two countries, Brazil and Mexico.

Up until now, over 100,000 people have created a secure account on the Better by Bowhead platform, including not only study participants but also digital health consumers who have come across the application on the Apple iOS and Google Play stores. The application has expanded to include 13 languages and has now processed over two million unique health data transactions in a production environment in compliance with Canadian, American, and European health data protection standards. The application is an innovative, user-friendly health data management platform that enables people to build their secure health databases or "data wallets" with self-reported daily health behaviors, digital biomarkers, validated questionnaires, and disease-related symptom surveys, with the ultimate goal of empowering people to improve their short- and long-term health. It also enables the tracking and sharing of medication-related data and uses incentive-based gamification mechanics to reward health tracking and data sharing on the application and nudge behavior change. Platform users may continue to contribute anonymous data toward real-world research, as well as connect with local specialists and patient communities to seek care. Upon sufficient data collection over time, machine learning algorithms could be created to feed personalized insights back to users to help with the prevention and early identification of disease. This feature is currently in development on the platform.

An extra mile While implementing the BHH platform, we attempted to use the platform for emerging public health issues. At the beginning of the COVID-19 pandemic, we decided to launch a privacy-first solution to help people and researchers better understand how the virus was spreading and evolving. We deployed a self-assessment tool and worked around the restrictions that the Google Play and iOS App stores were adding to COVID-19 tracking health apps by seeking an Independent Review Board (IRB) review, which we had previously worked with for our RWD studies. The IRB validated our solution and both stores gave us the green light to publish our application. In our case, having an application built on the

blockchain worked in our favor as we could easily disclose that all user data were anonymized and no personally identifiable information was stored in the system.

6 Implementation Learnings and Recommendations

Being in a nascent industry with few use cases meant that as a company, we had a steep learning curve. We experienced several challenges as we set out to build the Bowhead Health platform; by overcoming the challenges, we adapted our platform and accumulated learnings that may be generalizable to implementing blockchain-based health applications.

6.1 Learning 1: Gas Fee Needs to Be Minimized

In 2017, we analyzed the beneficial use cases of the blockchain in healthcare and implemented a proof-of-concept application focused on healthy habit tracking and data collection. In the planning phase, we analyzed the Waves blockchain as the basis for our platform as they promised support for smart contracts in the short term and had a growing community. Unfortunately, the implementation of the Waves protocol was not released within the promised deadline and we decided to use the most mature blockchain at that moment that supported smart contracts, which was the Ethereum blockchain. This was the first version of the Better by Bowhead application. One of the first obstacles we encountered was derived from the gas fee that is highly coupled with the Ethereum blockchain.

Gas is a mechanism created to incentivize miners to process and prioritize data transactions. It is a fee that everyone needs to pay to store data on the blockchain if we are deploying our solution on the Ethereum main net. It is paid using ether (ETH) which is Ethereum's native currency. Given the several health data points that could be tracked and managed daily, gas fees would be too high. For example, if a user was logging several events per day, these microtransactions may exceed $10 dollars per day, making it nearly impossible to scale. To incentivize platform usage, we needed to make it free for users, otherwise, it would be a competitive disadvantage compared to other similar solutions already in the market. We would therefore need to subsidize gas fees for users storing data on the blockchain, which would be an extraordinary expense for our company.

To solve this problem, we forked the Ethereum codebase and rebranded it with Bowhead's terminology which is tailored to health. This included the creation and naming of our native currency on the platform, called Anonymous Health Token (AHT). To keep gas prices low and under control, we were now able to specify that the gas price should be zero for all user transactions.

Upon overcoming the gas obstacle, we deployed our first minimum viable product (MVP) to the public and started adding features to showcase our platform capabilities.

6.2 Learning 2: User Experience Is Critical to the Success of a Digital Health Application and a Design-First Approach Is Important

The implementation of the BHH platform informed us that user experience is critical to the success of a digital health application, especially if the application is requesting near-daily interactions on the topic of personal health, which requires empowerment, originality, and trust. The onboarding experience, especially one that has multiple steps as in our case, must be simple, while also being informative so that users understand what sets our privacy-first health data-sharing platform apart from others in the market.

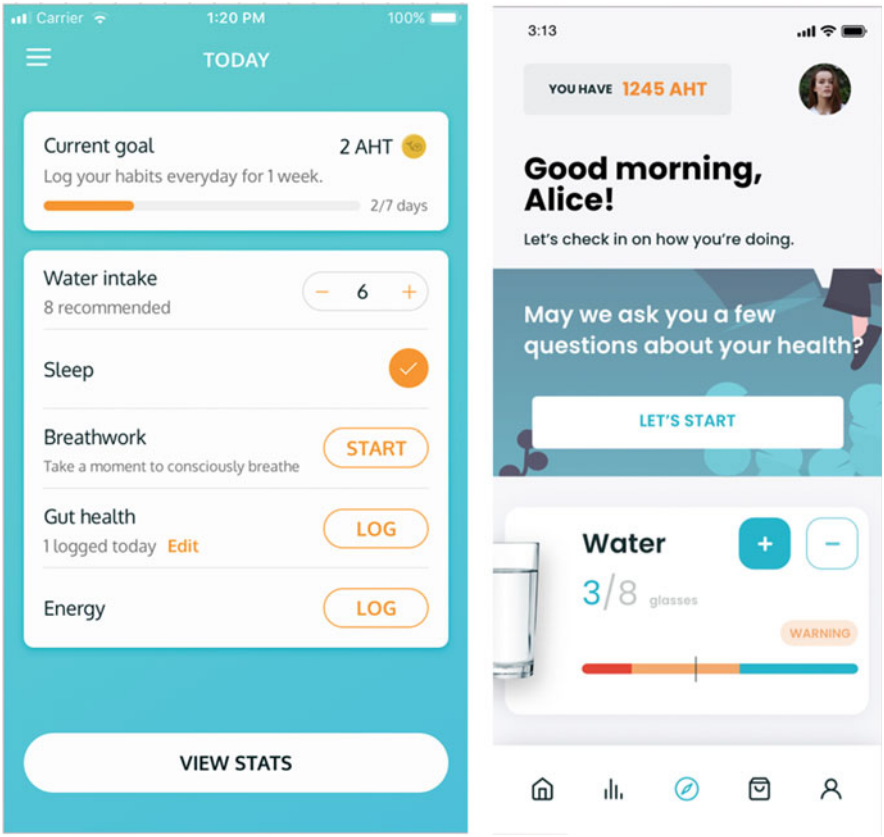
To ensure a sound user experience that resulted in retention, we followed a design-first approach. We created different versions of the onboarding experience and delivered them to our target users: females aged 20 to 30 years old. We focused on this group because it represented more than 60% of our platform's user base.

Upon testing our target customer, we learned that clean designs tied with graphical details, called micro-interactions, were more appealing to users and improved user engagement with longer form surveys. We also learned that users preferred simpler language versus scientific or technical terminology on the platform. We identified this preference when analyzing the funnels within our application. Around 30% of users dropped the onboarding process when they were presented with questions that contained specialized terms. Figure 4 illustrates how our user interface changed over time.

6.3 Learning 3: Economic Incentives May Not Be Appropriate for Health Applications

We hypothesized that providing economic rewards using the Bowhead blockchain's native currency—AHT and inviting patients to spend AHT toward health-related products in an in-application marketplace would result in more engagement with the application. However, this was not the case in reality.

We found that users could be grouped into two types: (1) prize driven, referring to users that are motivated to get free products and (2) not interested in the prize, referring to users not motivated by free products. These two types of users exhibited different responses to economic incentives (e.g., free products) that we offered. The first type added spam by tracking inputs not related to their daily activity. As a result, when we tried to analyze correlations between daily healthy habits and conditions, we did not find any meaningful pattern, except that they were tracking the needed data to earn precious AHT. For the second type, since they are not motivated by economic incentives, many of these users stopped tracking their daily health and uninstalled the app after some time.



MVP Design Current Design

Fig. 4 Evolution of User Experience. (a) MVP Design (b) Current Design

6.4 Learning 4: The Best Way to Retain Users Is by Helping Them Improve Their Lives

This learning lesson is related to Learning 3, as it was derived from the experience we had with our first attempt to add an economic layer using our blockchain currency and later reinforced when the application mechanics were analyzed by user experience researchers focused on health apps. The researchers compared our application against other reference applications by the number of downloads and ratings (Omberg, 2020; Park, 2022). Those applications with better retention and user satisfaction were those that prioritized health-promoting content.

6.5 Learning 5: Channels for Communicating with Users Must Be Established Within Blockchain-Based Health Applications

In traditional health applications, the application stores user information in central servers, such as emails and phone numbers, that allow convenient communication with users, despite the potential of revealing identifying information about the user. In a privacy-first application like the BHH platform, emails are non-existent, therefore extra steps and communication channels such as push notifications or in-app messages must be implemented to engage with users and improve user experience. For peak engagement, this requires the style of communication and language to be intentionally thought out.

6.6 Learning 6: Innovative Back-End Engineering Is Needed to Make User Experience Seamless

In traditional health applications, one common mechanism used to maintain a good user experience is called "sessions." These are used to identify a user who created an account and authorize the user to access an application. In this case, users can track and store data in the application and retrieve the data from any device as long as they have their account details on hand, which are commonly email and password.

In a decentralized ecosystem, however, this mechanism does not exist; instead, everything is handled by decentralized applications or dApps. Cryptography is used to generate a private key that acts as the user's account password and digital signature in smart contracts that manage data transfer and storage. As a result, authenticating users and retrieving their information from devices are considerably slower than sessions due to the Ethereum blockchain's previous consensus mechanism—proof of work, which could take about 10 minutes to store data in an application. This adds extra complexity from the application flow perspective, which means innovative "behind the scenes" back-end engineering is needed to make user experience seamless, more specifically, to allow users to perform in-application actions when user data is not being processed.

It is important to mention that Ethereum has changed its consensus mechanism to Proof of Stake, which has shortened the time to authenticate users on decentralized applications. Nevertheless, innovative back-end engineering is still needed for the speed of authenticating users on decentralized health applications to match traditional ones.

6.7 Learning 7: Storing Patients' Encrypted Data in Multiple Locations

To be compliant with privacy standards like GDPR, we improved our system by supporting the storage of the patient's encrypted data in multiple locations. We implemented this feature in a way that is transparent for the user and the researchers

while supporting different cloud providers from different locations. In this way, we were able to launch more studies, like the migraine and atopic dermatitis studies, while complying with strict standards.

6.8 Learning 8: Combining On-Chain and Off-Chain Storage

Abiding by GDPR also meant that a data service must grant users the ability to request data deletion amongst other policies. Using blockchain may seem counter-intuitive since an immutable record is created, oftentimes puzzling people as to how data is deleted if it is stored forever on-chain. By only using the blockchain to manage encryption keys and having the data stored off-chain in Interplanetary File System (IPFS) nodes, we could process the data deletion upon request.

6.9 Learning 9: Education and Advocacy Are Important for the Adoption of Blockchain-Based Health Applications

Our five-year experience in the blockchain industry suggests to us that blockchain is not only a technology but also a philosophy and ideology. In healthcare, blockchain serves to put patients and values first. As we realized that this might not be obvious to the majority of healthcare stakeholders, we launched an advocacy platform, podcast, and interview series during the pandemic focussed on the future of healthcare. We interviewed over 25 interdisciplinary global healthcare leaders championing values-based and patient-centric healthcare, aiming to join forces with fellow leaders to envision a better healthcare system for the digital age and learn about the various advancements in the industry including blockchain. The series was designed as a documentary-style audio experience that took listeners through 20-minute explorations of different areas where our healthcare system is evolving. Leaders were invited to slow down and reflect on how their work might be impacted by trends and tensions such as shifting consumer expectations, a rise in health data security breaches, and a movement toward community-centered healthcare delivery.

We believe that education and advocacy can help build trust with potential collaborators and partners for blockchain adoption to occur in healthcare. Once trust is established, adoption would follow.

7 Future Directions for Research and Implementation

Based on our learnings, we have envisaged the following directions for future research and implementation. First, it may be worthwhile to research and pilot the usage of soulbound tokens for user retention. During the implementation of the BHH platform, we learned that user retention is a major challenge beyond blockchain and more broadly affects most digital health applications. From a 100,000-patient study,

retention was on average 5.5 days (Omberg et al., 2020). This industry-wide challenge means that both start-up and multinational health organizations must find new ways of engaging and retaining users. Our studying of the blockchain industry, combined with first-hand experience in implementing a decentralized application, suggests that nonfungible tokens and soulbound tokens could be helpful ways to engage and retain users.

Soulbound tokens are blockchain-based transactions that are linked to an account and cannot be transferred. They could provide an elegant solution for gamification by having badges marked on a user's unique address. For example, after completing a 30-day streak of tracking healthy habits, a user could "mint" soulbound tokens and begin building a collection of noteworthy health events. The collection can then be used as evidence that qualifies users to participate in clinical studies, as described in the middle section of Fig. 5.

While experimenting with soulbound tokens, we also plan to take the BHH platform to the next level by transforming it into a platform where any organization can create studies, request data from users, and perform analysis using users' anonymous data. Certainly, the data will be only collected from users that are willing to share information for research and have given proper consent. Besides, we may offer a transparent audit trail by which anyone can assess how user data is treated. In addition, we intend to make BHH completely open source such that researchers, developers, and anybody interested can review the code, collaborate on projects, or even fork the platform. Lastly, we may engage the concept of Health-focused Decentralized Autonomous Organizations (HealthDAOs) to further empower patients to own their data and tokenize patient participation in the health breakthroughs of tomorrow. We are taking the first step in this direction by partnering with the dHealth Foundation—a non-profit organization that aims to advance decentralized healthcare through decentralized governance and patient engagement.

8 Conclusions

As we have shown, blockchain technology has the potential to improve healthcare research and delivery, while prioritizing patient safety and data sovereignty. Given this industry is at the early stage of development as we have described, the implementation of blockchain in healthcare has been a trial-error process and brought out several important learnings. By sharing the implementation of BHH and the learnings therein, we hope that implementors of the future can develop more user-friendly and sustainable applications that benefit the entire blockchain healthcare ecosystem.

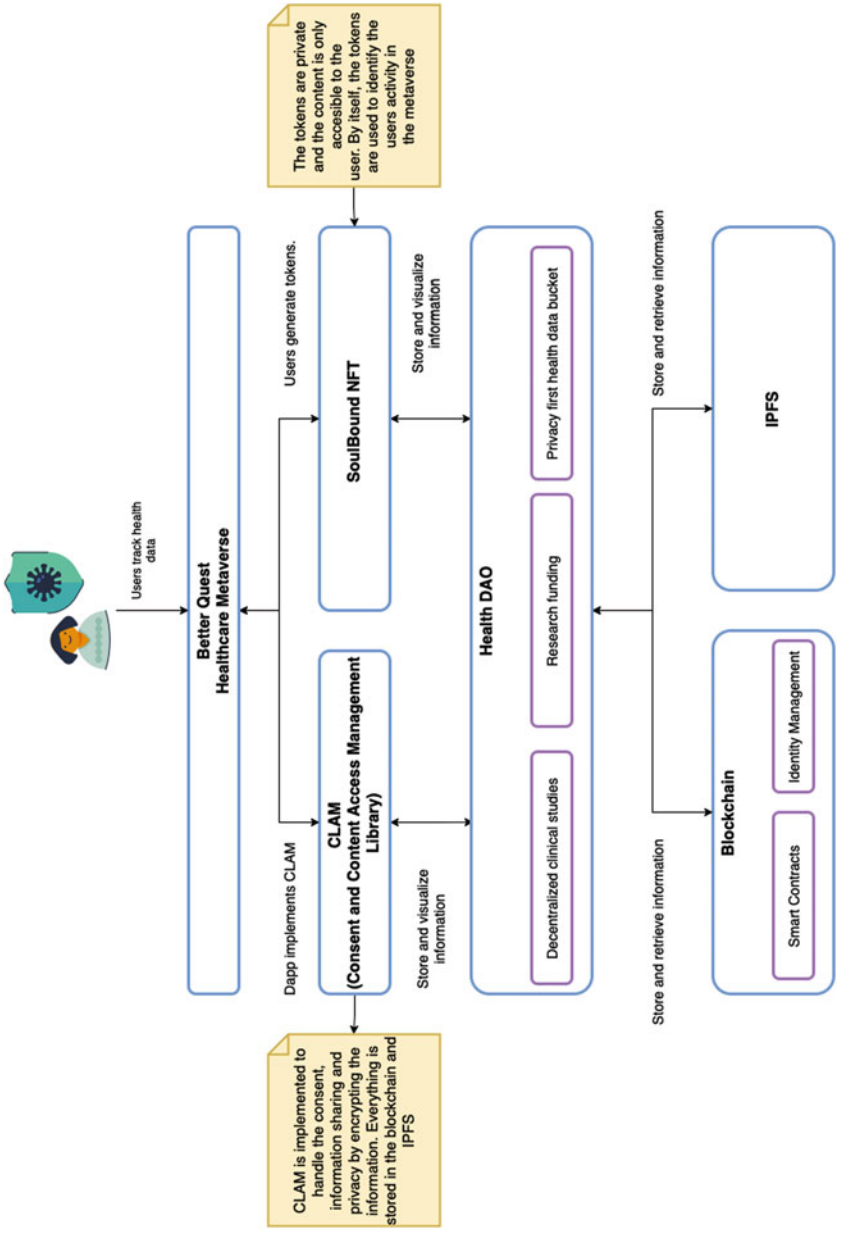


Fig. 5 An example of soulbound token usage in decentralized

References

Agrawal, R., & Prabakaran, S. (2020). Big data in digital healthcare: Lessons learned and recommendations for general practice. *Heredity, 124*, 525–534. https://doi.org/10.1038/s41437-020-0303-2

Ikeda S (2020). *Lifelabs data breach, the largest ever in Canada, may cost the company over $1 Billion in Class-Action Lawsuit*. Accessed Jan 8, 2020, from https://www.cpomagazine.com/cyber-security/lifelabs-data-breach-the-largest-ever-in-canada-may-cost-the-company-over-1-billion-in-class-action-lawsuit/

Kerekovska, A., Mircheva, I., & Mirchev, M. (2020). The academic viewpoint on patient data ownership in the context of big data: Scoping review. *Journal of Medical Internet Research, 22*(8), e22214. https://doi.org/10.2196/22214

Lucassen, A., Simon, D. A., & Liddell, K. (2021). Patient data ownership: Who owns your health? *Journal of Law and the Biosciences, 8*(2). https://doi.org/10.1093/jlb/lsab023

Omberg, L., Arean, P., Heagerty, P. J., et al. (2020). Indicators of retention in remote digital health studies: A cross-study evaluation of 100,000 participants. *NPJ Digital Medicine, 17*, 3–21. https://doi.org/10.1038/s41746-020-0224-8

Park, A. (2022). *Boehringer's digital rewards club boosts COPD medication adherence by 44%: study*. Accessed Aug 10, 2022, from https://www.fiercebiotech.com/medtech/boehringers-gamified-rewards-program-boosts-copd-medication-adherence-44-study

Roussanov, A., & Mulryne, J. (2021). *Regulatory and data privacy issues relating to real world evidence*. Accessed Sep 29, 2021, from https://thejournalofmhealth.com/regulatory-and-data-privacy-issues-relating-to-real-world-evidence/

Wikipedia. (2022). *Blockchain*. https://en.wikipedia.org/wiki/Blockchain

Wu, J., Qiao, J., Nicholas, S., Liu, Y., & Maitland, E. (2022). The challenge of healthcare big data to China's commercial health insurance industry: Evaluation and recommendations. *BMC Health Services Research, 22*, 1. https://doi.org/10.1186/s12913-022-08574-2

Co-founder and Head of Partnerships, Rhea Mehta, Ph.D., has been working at the intersection of science, digital health, and holistic medicine for over 10 years. She holds a Ph.D. in Molecular Toxicology from the Department of Pharmaceutical Sciences at the University of Toronto and a Bachelor of Science from the University of Waterloo, with over 15 scientific publications. Rhea is also a certified integrative health coach and has been operating an Optimal Health Coaching Practice and Consultancy for the past 10 years. Rhea currently sits on the industry advisory board of McGill's Masters of Management in Analytics Program.

CEO and Co-founder, Francisco Diaz-Mitoma Jr. is a lifelong technology architect specializing in privacy and user design with over 15 years of experience building scalable technology. His expertise is in building privacy-by-design frameworks and connecting these innovations with leading health researchers. Francisco graduated from McGill University in Political Science and has been honored as a Forbes 30 under 30 for his previous work in gaming and online advertising.

As CTO, Cesar Diaz has more than 15 years of experience working on software projects. One of his passions is creating projects from scratch, articulating the entire pipeline, beginning with pitching the idea and finishing with customer support. He is an open-source advocate, a builder of Smart Contracts, a contributor to the security-focused software community, and continues to look for new things to discover. He graduated from Universidad del Valle de Atemajac in Software Engineering and to this day tries to improve the world through lines of code.

The Inter-Organizational Environment of Blockchain in Healthcare: The State of Blockchain Healthcare Consortia

Trinh Nguyen-Phan and Chang Lu

Abstract

Investment and attention to blockchain burgeoned since 2019 and healthcare is one active industry experimenting with this novel technology. Among the projects in the healthcare blockchain sphere, the most prevalent theme is the booming of healthcare blockchain consortia. To explore the growing partnership activities in the healthcare blockchain sphere, we conducted a content analysis of collected archival data from public sources to address two research questions: *What are these healthcare blockchain consortia and what are the potential benefits and challenges to these consortia?* We found that healthcare organizations activities in forming consortia are largely unstructured. Information about their members, visions, objectives, and agenda is fragmentary, elusive, and sometimes confusing; most consortia are small size with less than or equal to 5 members and most organization join one consortia. Insights from strategic alliances and the emerging blockchain governance literature suggest that these consortia might face several organizational challenges to mature, especially when they are not prepared for the novel decentralized governance of blockchain consortia.

1 Introduction

This chapter was initially a report of a Mitacs Accelerate Internship done in the fall of 2019 when blockchain investment and discussion burgeoned. The year 2019 also marked the momentum of blockchain research. However, academic research in blockchain up to that time chiefly focused on the technical concerns such as

T. Nguyen-Phan (✉) · C. Lu
The School of Information, University of British Columbia, Vancouver, Canada
e-mail: trinh@student.ubc.ca; chang.lu@ubc.ca

C. Lu, M. Tanniru (eds.), *Blockchain in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-031-45339-7_9

consensus mechanism and cryptography. Studies exploring blockchain from an organizational and strategic management perspective were scant. Among many industries experimenting with this novel technology, healthcare was hailed as one of the most prominent applications of blockchain (Tapscott & Tapscott, 2016; Vigna & Casey, 2018). Despite the hype around blockchain projects, however, very little is known about what healthcare organizations are doing in their blockchain endeavor and how they go about it.

Using archival news searching on public news site (Coindesk and Google) and content analysis, we were able to identify that most healthcare organizations were forming partnerships or consortia for their blockchain projects. In particular, we searched the term "healthcare" in coindesk.com—a popular news website specializing in blockchain—and analyzed all available articles loaded in the website. This detected 232 articles with the first article dated 17 October 2013 and the most recent article was released on 14 August 2019 as of September 2019. Among 232 collected articles, 88 were directly relevant to blockchain application in healthcare. The top activities of organization in the healthcare industry include forming blockchain partnerships or consortia (28/88 articles), research (18/88), record management (12/88), payment application (9/88), and fund raising (8/88).

The growing trend in forming healthcare blockchain consortia resonates with both blockchain academic researcher and industry consultant. For instance, Clauson acclaimed that blockchain consortia is a crucial strategy for exploring blockchain for healthcare (Clauson, 2019). Deloitte—an active advocate of blockchain—identified expansion of consortia as one of the five key vectors that could drive wider adoption of blockchain (Deloitte, 2018). Deloitte's 2019 Global Blockchain Survey also reports that 92% of the respondents say they either belong to a consortia or plan to join one in the next 12 months (Deloitte, 2019a). Nonetheless, information about these healthcare blockchain consortia was fragmented and elusive. This study therefore sought to answer two questions: *What are these healthcare blockchain consortia and what are the potential benefits and challenges to these consortia?*

Since literature on blockchain technology was only beginning to emerge in 2019, and the literature on healthcare blockchain consortia is even more sparse, we used strategic alliances literature for a theoretical reference to discern the trend, opportunities, and risks of the rising healthcare blockchain consortia. The strategic alliances research provides several empirical evidence that can be transferrable to healthcare blockchain consortia. In terms of benefits, consortia membership might enhance cost savings and knowledge exchange. On the other hand, it also requires tremendous effort by member organizations. At a tactical level, the so-called coopetition nature of consortia comes with many important considerations regarding the consortia's goals and objectives, governance model, funding, staffing, and decision-making (Deloitte, 2019b). Academic research also provides a plethora of studies about the major roadblocks to interorganizational partnership. Hence, the benefits of joining consortia are not innate but must be realized with deliberate thinking, planning, and executing.

Yet, as blockchain is a novel governance paradigm, the traditional strategic alliances management models were rather a useful reference, but not a tool

specialized for organizational strategy under the blockchain era. With the opportunity to reproduce this report into a book chapter in 2022, we now integrate contemporary research into our literature and findings. In three years, much has evolved in the blockchain sphere. There are many more research from various disciplines, adding considerable nuances in understanding about blockchain. This chapter is now incorporated with the emerging literature of blockchain governance that was not available at the report's inception.

Reflecting on the theoretical, the findings suggest the need to diversify the membership within healthcare blockchain consortia and interoperate between consortia to better realize strategic alliances benefits. This insight in turn resonates with the call for more understanding in the digital ecosystem and blockchain governance.

2 Review of Strategic Alliances Literature

At the time of the research project in 2019, there is not yet a specific literature on blockchain consortia, so we explored the broader landscape of research on strategic alliances. The theoretical frameworks of strategic alliances research form the foundation for our critiques of the movement of healthcare blockchain consortia. Until 2022, we still find these insights and critics relevant to the human governance part of blockchain consortia, especially in the early stage.

Our review of the strategic alliances literature addresses the definition, benefits, challenges of consortia, and measures of success for joining a consortia. As this article focuses on consortia of organizations, the terms strategic alliances, consortia, and partnership are used interchangeably.

2.1 Benefits of Collaboration

Strategic alliance, collaboration, or partnership refers to a purposive relationship between two or more independent organizations that pool in resources or capabilities to achieve mutually relevant benefits (Gulati, 1995). The literature has varied typology to classify different types of alliances. Consortia is considered the most sophisticated type of strategic alliance (Lei & Slocum, 1991). The consortia model is designed to maximize the benefits of joint ventures while allowing for organizational specialization and is well developed in several countries. Consortia is not exclusively a Western concept, the Japanese model of consortia is called *keirestsus* and the Korean's is *chaebols* though they may vary in terms of structures, members, and capital source (Lei & Slocum, 1991).

Companies may engage in one or more strategic alliances for reasons beyond economic benefits such as self-interest toward legitimacy or moral rationale. Legitimacy drives partnering activities with one or more desired partners to gain visibility for political lobbying, public relations management, or brand building, whereas a moral mission encourages multi-organizational collaborations to address societal

issues—poverty, crime, hunger—that are impossible for any single organization to solve (Huxham, 1996, pp. 3–4).

In term of economics, key benefits of inter-firm collaboration comprise effectiveness and efficiencies (Lei & Slocum, 1991). Effectiveness is the most compelling rationale for firms to engage in strategic alliances. Effectiveness is achieved when firms involve collaborate rather than simply exchange (Kanter, 1994). Partnerships succeed when organizations collaboratively provide complementary expertise, knowledge, technologies, and resources to tackle common problems that are beyond the capability of any single firm to solve (Huxham, 1996; Kanter, 1994). On the other hand, interorganizational partnership is weak and less sustainable when firms simply pool similar resources to produce a single product or services (Kanter, 1994). Effectiveness is particularly realized in R&D consortia when innovation resides in networks of learning rather than within an individual organization. Put differently, R&D consortia are particularly beneficial to members when engaging with complex and expanding knowledge, when individual firms have discreet expertise and resources, and when the pathway for technology development is highly uncertain. A study of the US biotechnology sectors corroborated this, as firms with a dense network of alliances grew faster than did those without such a network (Powell et al., 1996).

Efficiency is the second economic reason driving organizations to work together. Incentives for collaboration include economies of scale, risk sharing, reduced duplication of effort, and access to new market and technologies (Lei & Slocum, 1991). Efficiency is particularly valuable in resource-scarce situations when collective efforts are predicted to resolve duplication and improve economic advantage (Huxham, 1996; Lei & Slocum, 1991). Often R&D alliances provide a venue for government support, as in the United States and Japan, to augment international competitiveness in critical industries (Ouchi, 1989). Two pragmatic observations, nonetheless, circumscribe the credence of the value of R&D collaboration. First, research in the USA and Japan suggest that private sector R&D consortia are more likely to focus on lower priority problems, short-term gain, and incremental research rather than long-term and radical innovation (Ouchi, 1989). Second, collaborative arrangements do not tend to lead to cost-reduction, and cost-reduction per se is insufficient to sustain a productive collaboration (Huxham, 1996; Kanter, 1994).

Alliances can also be used to offset the adjustment costs during a nascent period of industry change (Eklund & Kapoor, 2019). Adjustment costs refer to the costs that arise in the early stage of industry change due to turbulence between the old and the new business models and during the period of uncertainty as to which model will prevail. These costs consist of direct costs associated with the development of human resources, assets, technologies, and routines to support the new model as well as the indirect costs associated with the disruption to the existing models via sharing of resources and managerial attention. Eklund and Kapoor's study of the U.S electric utility industry suggests that firms partnering with alliances from outside industry mitigate adjustment costs and that their pursuit of the new model is associated with higher firm valuations when it is undertaken via alliances than when it is undertaken in-house (Eklund & Kapoor, 2019).

2.2 Challenges of Collaboration

Despite the strong advocacy for strategic alliances by arguments of legitimacy, social responsibility, effectiveness, and efficiency, interorganizational collaboration is far from a low-hanging fruit; over 40% of partners report that they are very dissatisfied with the results of their collaborations (Bleeke & Ernst, 1993). Alliance management is inherently difficult due to the very nature of alliances: first, two or more firms, often with competing interests and expectations, working together to achieve a particular outcome; and second, decision-making, which is often difficult within a firm, must now be achieved among organizations (Deloitte, 2019b). Hence, Huxham (1996) contends that collaboration is more time- and resource-consuming than non-collaborative activities.

The reasons for alliance dissatisfaction classify into four groups: *collaborative inertia* that slows down the pace of work and decision-making and increases resource consumption (Huxham, 1996); *sharing of control* as a trade-off for gaining access to complementary skills and knowledge (Gomes-Casseres, 1993); *power differences* that permit some partners to capture a larger proportion of the collaboration outcomes (Porter, 1986); and *differences among organizations* regarding the purpose for collaboration as well as in organizational culture and values (Huxham, 1996; Kanter, 1994; Mattessich & Monsey, 1992). These differences ultimately lead to lack of trust, conflicting agendas, and degradation of staff commitment and, consequently, undermine the time, costs, efforts, and management of alliances (Gray, 1989).

2.3 Success Factors for Collaboration

Interorganizational collaboration involves a myriad advantages and disadvantages; yet, it is believed that "the progressive companies now put the alliance activities in the heart of their strategy" (Duysters et al., 1999, p. 346). It is important, therefore, to understand the critical factors that influence the success of alliances. From the literature of strategic alliances, we identify three key ingredients for a successful partnership.

First, the motive for partnership should be built on a collaboration in which parties pool complementary skills, knowledge, and resources to achieve a common goal. Organizational members should be aware of the resources that it takes for an effectiveness-driven partnership; collaborative work with the intention of reducing costs is more likely to fail. Organizations should only consider collaborations that help each organization achieve a priority that no single firm, acting alone, can achieve (Huxham, 1996). To this end, the goal of the partnership should be clear and transparent.

Second, there must be trust between partner members (Duysters et al., 1999). Trust is foundational to the formation and maintenance of partnership (Bergquist et al., 1995). Bergquist et al. (1995) articulate trust in three dimensions: *trust in intentions* that occurs when the members believe that they are pursuing the same

objective and will not hurt the interests of the others, *trust in competency* that occurs when the members believe each partner has the necessary skills, knowledge, and ability to deliver, and *trust in perceptions* that occurs when the members believe that they are standing on the same ground and looking at the same direction. Merrill-Sands and Sheridan (1996, p. 8) assert that "without respect and trust, it is impossible to move forward on any joint agenda."

Third, managing alliances skill is the engine of a successful partnership. Bleeke and Ernst (1993) suggest that a paucity of management skills can drive the alliances into serious managerial and financial troubles within the first 2 years. Kale and Singh (2009) champion management capability for alliances as a competitive advantage in a world in which firms increasingly rely on alliances. They advocate for "alliances portfolio management" because organizations now commonly engage in multiple alliances instead of the conventional one-on-one relationship. The portfolio approach differs from regular alliance management as a firm's alliance portfolio capability requires more sophisticated arrangement of complete, non-competitive, and complementary sets of alliances. The focal firm also needs to ensure maintenance and support of trust and collaboration across different partners in the portfolio and coordinate among strategies and operations across alliances in the portfolio.

In summary, managing effective alliances is at best, challenging, and at worst, likely to collapse. Building effective alliance capability may take between 5–10 years (Kale & Singh, 2009) and failure rate can be as high as 50–60% (Duysters et al., 1999). To maintain their relevance in the industry, however, firms cannot afford to omit partnering with other organizations (Duysters et al., 1999). First, the world has experienced an unprecedented growth of technology, competition, and uncertainty; so, firms need to hedge themselves against this turbulence by partnering with competent partners (Duysters et al., 1999). Second, the competitive landscape has profoundly shifted from the individual level to the network level. Firms now form networks with competitors to compete with other similar networks (Duysters et al., 1999).

Strategic alliances is a highly dynamic domain requiring firms to evolve constantly their partnership approach to adapt to the changing business environment. In the 1960s, firms merely used alliances to gain access to new markets or to bypass government regulations (Duysters et al., 1999). By the turn of the twenty-first century, alliances were a central part of most firms' strategies (Kale & Singh, 2009). In a report by Partner Alliances, more than 80% of Fortune 1000 CEOs believed that alliances accounted for almost 26% of their companies' revenues in 2007–2009 (Kale et al., 2009). In the past three years, the nascent blockchain technology has drawn hundreds of organizations in different sectors together in consortia, escalating the unpredictability of these partnership due to high level of uncertainty in both interorganizational alliances and blockchain technology development. This grants urgency to the study of the current state, potential challenges, and complexities associated with healthcare blockchain consortia.

3 Methodology

Given the limited theory and evidence, we chose an explorative, qualitative approach (Berg, 1954; Eisenhardt et al., 2016). Our setting is the consortia of blockchain in healthcare sector. Our study can be divided into two phases that in combination provide the breadth and depth of data for content analysis. The first phase focuses on the breadth of data collection, aiming to scan through the public news to consolidate an exhaustive list of current healthcare blockchain consortia. The second phase focuses on the depth of data in each consortia.

In the first phase, we collected online archives about consortia of blockchain in healthcare aiming for an exhaustive list of current healthcare blockchain consortia. We collected data from Google search using the combinations of the term *healthcare blockchain* with each of the following terms *consortium, consortia, collaborative, collaboration, initiatives, partnership,* and *alliances*. After that, we reviewed the effectiveness of our search terms and decided that *"consortia*" resulted in the highest relevancy. We then extended our search for healthcare sector by using other related terms, including *pharma blockchain consortia* and *life sciences blockchain consortia*. For every search term, we then read through all displayed results in the first three pages of search results and recorded relevant information, excluding sponsored advertisement. A piece of information is considered relevant if it explicitly mentions at least one specific name of a healthcare blockchain consortia. One-on-one partnerships, which we occasionally encountered during data collection, were not counted as consortia. The result is a total of *27 Google search result pages containing 197 unique URLs* excluding sponsored advertisement. Each article was coded with its respective Search term, Date (of search), Result URL, Page number (1, 2, or 3), Relevance (yes or no), Duplicate (yes or no), and a Note of how relevant the article is to our search purpose (Fig. 1). If an article is Relevant and Not Duplicate, we recorded the name of the mentioned consortia/consortia in a separate sheet for the next step.

Search term	Date	Result URL	Page #	Relevance	Duplicate	Note
Healthcare blockchain consortium	27-Dec-19	https://hashedhealth.com/consortia-july-2019-2/	1	Yes	No	7 major consortia
Healthcare blockchain consortia	27-Dec-19	https://www.forbes.com/sites/chrissamcfarlane/2019/03/14/health-care-and-blockchain-the-impact-of-consortia/#450207335b16	1	Yes	Yes	3 consortia, 2 already mentioned in 7 major consortia by Hashed Health

Fig. 1 Excerpt of a record of data collection

In the second step, we conducted a Google search for each of the recorded consortia to collect information about year of establishment, key members, members' industry, goal, and the consortia's communication media (website, social network channels). In this step, the search was purposeful; we used a wide variety of key words such as *"founding date of x consortia," "members of x consortia," "x consortia partner with"* to search for the desired information. We skimmed through the first page of results and constantly adapted our search terms until we reached a saturation of information, meaning other articles did not provide new information. Finally, we used content analysis techniques to compare information across the consortia to find the patterns of operation and from that, inferred the potential success factors and challenges.

As this is an exploratory-archival data collecting method, we assessed the quality of our data by comparing our result with a paid-report from ESG Intelligence, a private firm providing data on blockchain project and blockchain consortia. They used similar data collection methods of manual searching, filtering, and collating data from public sources. The result shows minor differences between our search and ESG report; namely, the ESG report included 5 consortia that we did not have, and we included 6 consortia that ESG did not. Among the 5 consortia that we did not include, one focused on the retail sector (with membership of one pharmaceutical company), one focused on federated learning rather than blockchain, and three advertised themselves as a "group project" or an "initiative" rather than a consortia. We decided, therefore, to retain our original list without altering our search terms.

4 Findings

4.1 The Immature Born of Many Blockchain Consortia

Healthcare blockchain consortia have been mushrooming since 2017, which was deemed an "unstructured experimentation of blockchain solutions" (Carson et al., 2018). Information about these consortia, however, is fragmentary and unconventional. Most news or press releases did not come from orthodox business news hubs like CNBC, Bloomberg, Reuters, or Forbes; they instead appeared in blockchain-specialized sites like coindesk.com and ledgerinsights.com or the newsletters of private firms or consortia. There is no single public source that seems to aggregate global information about existing consortia for application of blockchain in the healthcare sector. The most comprehensive source was the newsletter prepared by John Bass, founder and CEO of Hashed Health (Bass, 2019). Hashed Health is a healthcare blockchain innovation firm that is also the organizing force of the Professional Credentials Exchange consortia (usually referred to as Hashed Health or ProCredEx). Hash Health's list focused on the USA more than other regions; therefore, it does not capture the full picture of global healthcare blockchain consortia. The fragmentary news about healthcare blockchain consortia implies a high risk for data errors and for immaturity of partnership initiatives. For example, Health

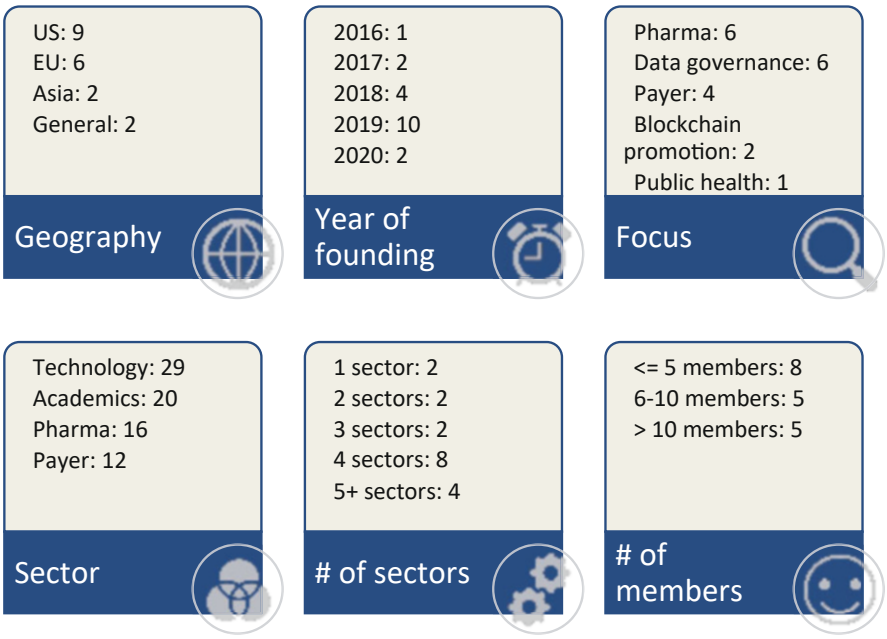


Fig. 2 Summary features of 19 healthcare blockchain consortia

Utility Network consortia, organized by IBM, does not have its own website to officially communicate its progress with the public.

Our initial data collection identified a total of 18 healthcare blockchain consortia whose details are presented in the following tables. During the writing of this book chapter in the summer of 2022, we implement the same search mechanism (this time we only search the term "healthcare blockchain consortia" on Google and review search result in the first 3 pages) and identify a new healthcare blockchain consortia, the PHBC (Public Health Blockchain Consortia). The PHBC was born in the Covid-19 era, making it the only healthcare blockchain consortia that focuses on public health, specifically on the use of health records. This increases the identified healthcare blockchain consortia to 19. PHBC and its administering company has their office in Belgium and the Netherlands. It defines itself as a consortia of health authorities, universities, health care providers and innovators (PHBC, n.d.). However, more specific information about its official members, protocol, and use case is not available.

A summary of each consortia's features is presented below (Fig. 2):

In general, the growth of healthcare blockchain consortia since 2018, chiefly focused on developed countries, and driven by private firms. In the total of 19 identified healthcare blockchain consortia, 16 ones have been established between 2017 and 2019. The year 2019 alone accounts for the inception of 10 of 19 healthcare blockchain consortia. The United States is home for more than one half of the healthcare blockchain consortia, followed by the EU (5 out of 19) and Asia

(2 out of 19). No identified consortia originate in Africa. These 19 healthcare blockchain consortia encompass more than a hundred organizations in 11 different sectors and include both healthcare and non-healthcare members. The latter include distribution (Walmart), bank (PNC Bank), academic institutions, and government agencies. Technology is the leading membership in these consortia with 29 technical partners, followed by academia (20 institutions and universities), pharmaceutical companies (16 organizations), and insurance companies (12 organizations). Data governance and pharmaceuticals-focused are two major focus of healthcare blockchain consortia.

There are a few noteworthy characteristics of membership composition in the consortia. Among more than 100 individual organizations, 90% of them join a single consortia. Merck was most active having membership in three consortia, namely, Mellody, the research consortia of FDA (US Food and Drug Administration), and SAP Pharmaceuticals and Life Sciences Industries Consortia. Although there are 11 identified sectors in these 19 healthcare blockchain consortia, most consortia consisted of only 1 to 5 sectors. The two consortia which had members from a single sector were the academic consortia and the NGO consortia, which focused on not-for-profit research promoting blockchain. Most healthcare blockchain consortia had members from 4 different sectors arranged around one or more technical partners. The average number of declared and notable organizational partners is 7 organizations. Half of the consortia had less than or equal to 5 members emphasizing the role of small consortia. Mellody and PharmaLedger were the two largest identified consortia with 17 and 25 members, respectively, spanning in several industries: pharmaceuticals, technology, NGOs, healthcare institutions, and academia (Fig. 3).

4.2 Myriad Challenges to Managing Healthcare Blockchain Consortia

The mushrooming formation of healthcare blockchain consortia in 2019 has, on the one hand, unequivocally reflected organizational attention to this emerging technology. On the other hand, it implies two major challenges to the success factors of strategic alliances from a traditional strategic alliances perspective.

First, the goal of partnership for many consortia is ambiguous. The "blockchain consortia" conflate permissioned interorganizational blockchain networks and collaborative alliances. In this context, any interorganizational project could announce itself as consortia without a clear statement of the collaborative vision and goals; this is detrimental to the development of the consortia. For instance, one can question the viability of single sector consortia such as the International AI and Blockchain Consortia (iABC)—comprised of the Asia University and the China Medical University sponsored by The Ministry of Science and Technology in Taiwan—and Pistoia Alliance Blockchain Initiative—comprised of four leading pharmaceutical companies in Europe without any notable partners in other sectors.

No.	Consortia name	Launch date	Focal country	# of Notable partners	Notable partners	Goal
1	**Synaptic Alliance**	02-Apr-18	US	7	Optum, United, Humana, Quest, Multiplan, Aetna, Ascension	to build a permissioned blockchain that would let members view, input, validate, update and audit non-proprietary provider data within the network, with the goal of improving data accuracy and lowering the associated administrative burden and costs.
2	**Hashed Health**	08-Nov-18	US	8	Wellcare, Anthem NGS, Spectrum Health, Accenture, Healthlink Dimensions, Hardenbergh Group, Texas Hospital Association, Hashed Health	to create a new business model for accelerated credentialing
3	**Health Utility Network**	24-Jan-19	US	7	IBM, Aetna, Anthem, HCSC, Cigna, PNC, Sentara	to allow the blockchain network to enable healthcare companies to build, share and deploy solutions that drive digital transformation in the industry.
4	**Coalesce**	17-Apr-19	US	4	NASCO, Express Scripts, Blue Cross Blue Shield, Horizon Healthcare Services Inc.	to improve the efficiency and accuracy of member healthcare data exchanges across entities within the Blues' ecosystem.
5	**Rymedi**	25-Apr-19	US	7	Rymedi, Temptime/Zebra, Indiana University Health, WakeMed Health, Good Shepherd, Center for Supply Chain Studies, Global Health Policy Institute	to track and verify specialty prescription drugs, to ensure safety, enhance value and improve health outcomes.
6	**MediLedger**	02-May-19	US	11	Pfizer Inc., McKesson Corporation, AmerisourceBergen Corporation, Genentech, Gilead, Walmart. Partners: Pwc, Deloitte, Cumberland, ISG. Organizer: Chronicled	to bring together leading Pharmaceutical Manufacturers and Distributors using an advanced and customizable decentralized supply chain management system based on the principles of blockchain.
7	**Mellody**	01-Jun-19	EU	17	Amgen, Astella, AstraZeneca, Bayer, Boehringer Intelheim, Gsk, Janssen, Merck, Novartis, Servier, Muegyetem 1782 (The Budapest University of Technology and Economics (BME)), Iktos, Ku Leuven, Loodse, Nvidia, Owkin, Substra Foundation	to establish a machine learning platform that would make it possible to learn from multiple sets of proprietary data while respecting their highly confidential nature
8	**RemediChain**	01-Jun-19	US	5	Lipscomb University, FedEx Institute of Technology at the University of Memphis, RemidiChain, FDA, Good Shephard Pharmacy	to use blockchain as a means to retrieve unused, high-value medications from patients and pass them on to economically disadvantaged patients who would not be able to regularly afford them.
9	**FDA (US Food and Drug Administration)**	07-Feb-19	US	5	FDA, IBM, Merck, Walmart and KPMG	to test new technologies that can help trace and verify prescription drugs in the United States
10	**Embleema Health Blockchain Consortia**	2017	France, US	13	The Government of Armenia, WHISE, Janssen, Harvard University, Servier, Techstars, Pierre Fabre, Hyperledger, PharmaGest, The George Washington University, IEEE, Gustave Roussy Institut, Embleema	to give back the ownership of data to patients, and securely connect the major stakeholders in the healthcare industry together; biopharma, hospitals, doctors and patients through blockchain technology.

Fig. 3 List of 19 healthcare blockchain consortia

11	**Blockchain in Healthcare Global (BiHG)**	Q1-2019	Global	5	Consensys Health, AMSYS, simplyvital health, Decent, Rymedi	to mitigate the barriers to adoption of blockchain in healthcare and research and to empower clinicians, patients, and administrators and life science researchers to improve outcomes with blockchain and converging technology.
12	**UK-India consortia**	14-Aug-17	Global	2	City University London, Indian Institute of Technology Kharagpur	to explore the use of a privacy-preserving blockchain architecture for IoT applications in healthcare data-sharing, using attribute-based encryption (ABE) to provide greater security for the devices
13	**International AI and Blockchain Consortia (iABC)**	Jan-18	Taiwan - China	3	The Ministry of Science and Technology in Taiwan, Asia University, and China Medical University	to formulate an ecosystem that bridges the healthcare industry and domestic and international researchers
14	**MyData project**	16-May-19	South Korea	6	South Korean Government, MediBloc, Samsung Fire & Marine Insurance, Seoul National University Hospital, CHA University Hospital, and WELT	to strengthen the individual's right to self-determination and to help the individual who is the owner of the data to receive his or her own information or allow third parties to use it.
15	**My Health My Data**	07-Nov-16	EU	14	Lynkeus, Athena, IEIIT-CNR (National Research Council of Italy), Digi.me, Gnúbila, HES-SO (University of Applied Sciences Western Switzerland), Panetta & Associati, SBA Research, Siemens Healthineers, Transilvania University of Brașov, The Charité – Universitätsmedizin Berlin, Bambino Gesù Hospital, Queen Mary University London, University College of London	to build a blockchain-based software infrastructure in which individual data exchanges are governed by peer-to-peer relationships between all the stakeholders
16	**SAP Pharmaceuticals and Life Sciences Industries Consortia**	03-Oct-18	US	5	SAP, Merck, GlaxoSmithKline, AmerisourceBergen, and Boehringer Ingelheim	to provide a blockchain-based solution that will help to track and authenticate pharmaceutical packaging returned from hospitals and pharmacies to wholesalers before product are resold.
17	**Pistoia Alliance Blockchain Initiative**	06-Feb-19	EU	4	AstraZeneca, GSK, Novartis, and Pfizer	to use blockchain technology to improve data sharing, data identity and data integrity in the life sciences industry.
18	**PharmaLedger**	15-Jan-20	EU	29	12 global pharmaceutical companies and 17 other organizations spanning hospitals, universities, legal firms, and software development companies	to provide a widely trusted platform that supports the design and adoption of blockchain-enabled healthcare solutions while accelerating delivery of innovation
19	**Public Health Blockchain Consortia (PHBC) or the Virusblockchain**	19-Mar-20	EU	N/A	health authorities, universities, health care providers and innovators	To improve public health.

Fig. 3 (continued)

Some consortia are initiated by a single firm and therefore, named after the pioneer companies such as Rymedi, RemediChain, Hashed Health, and SAP. This potentially confounds the identity and agenda of the collaboration with that of the founding firm and might consequently impede member organizations' trust on one another. Contributing to this issue is the fragmentation and paucity of public communication regarding healthcare blockchain consortia, which can be understood due to either business confidentiality or short timeframe.

Second, the burgeoning healthcare blockchain consortia may have side effects on effective alliances management. Almost one half of the identified healthcare blockchain consortia do not have their own websites, leading to confusion in public news. For instance, the news on *managedhealthcareexecutive.com* mistakenly named Medibloc as one of the major blockchain consortia, whereas it is a private firm and member of MyData Project consortia (MediBloc, 2019; Walker, 2019). Those who have their websites do not usually keep it the most up to date. For example, MediLedger, despite being one of the most well-established consortia in terms of membership and public media coverage, has not updated the joining of Walmart in June 3, 2019 on its website (checked on January 17, 2020). Mellody, the largest consortia in terms of the number of members, launched its website 6 months after official establishment. It is particularly challenging to gather sufficient information regarding participating members, funding, and agenda for each consortia as this is scattered among many news articles. The absence of funding information questions the sustainability of many consortia as substantial resource investment in collaborative activities is key to successful strategic alliances (Gray, 1989; Huxham, 1996; Kanter, 1994). A shortage of skills in managing alliances, "main engine of successful partnership," has the potential to drag many current consortia down the road of serious managerial and financial troubles (Bleeke & Ernst, 1993).

4.3 The Missing Part of Blockchain Consortia Governance Puzzle: The Human–Algorithms Collaboration

Notwithstanding the important insights that the strategic alliances management models offer for blockchain consortia, they overlook the essence of the blockchain era: the decentralization of governance powered by algorithms. Traditional strategic alliances management models chiefly focus on singular focal organization. They are based on the assumption that humans are the only agents managing the system, reflected from the emphasis on (human) trust between organizations and the key considerations for successful strategic alliances management.

In 2008, an anonymous author or group known as Satoshi Nakamoto published a white paper detailing the creation of Bitcoin, a peer-to-peer digital cash system (Nakamoto, 2008). This innovative decentralized technology has since inspired numerous industries, challenging the sustainability of traditional centralized models (Tapscott & Tapscott, 2016; Vigna & Casey, 2015, 2018). Trust is still a vital element of blockchain, yet trust is now decentralized; it not only departs from the central third party but also from human actors to machine and algorithms (Vigna & Casey, 2018). Thus, the conventional assumptions about centralized trust is increasingly outdated (Seidel, 2017). An empirical example of this decentralized trust is the establishment of The DAO (Decentralized Autonomous Organization)—a hundreds of millions corporation—in 2016 with no legal authority, no government agency, and no corporate bylaws; trust in The DAO resided on the codes of "smart contract" written on the Ethereum blockchain (Banon, 2016). The DAO is also a

notorious example since The DAO attack in the same year resulted in a hard fork that separated the Ethereum and the Classic Ethereum blockchain (Siegel, 2016).

Despite "The DAO" failed experiment, blockchain has arguably introduced a novel governance framework, combining the human and machine actors in its governance (Lemieux & Feng, 2021). A large body of work in blockchain governance emphasizes the algorithmic governance aspect to design the protocol, system standards, and consensus mechanism as presented in the systematic literature review by Tan et al. (Tan et al., 2022). Blockchain purists go so far to proclaim that "code is law" and do not compromise even if this fixity drained out their investment, exemplified by the DAO attack in 2016 (Siegel, 2016). Nevertheless, the utopia "code is law" might only be achievable in a high trust and stable social environments (Lemieux & Feng, 2021). The reality is that these technologies are emerging and evolving, thus blockchain governance is also evolving (Lemieux et al., 2019; Lewis, 2021; Tapscott & Tapscott, 2016; Vigna & Casey, 2018). Understanding the evolving nature and being able to adapt the collaborative governance between algorithms and humans are crucial to successful blockchain initiatives (Goldsby & Hanisch, 2022) (Rikken et al., 2019).

To be clear, the collaboration of algorithmic governance and human governance does not discount the steering role of the human actors in the governance of blockchain consortia. One may argue that the forming and management of the blockchain consortia themselves are purely human-driven, and the algorithmic governance is not relevant at this stage. However, decisions at this stage of governance (for example, whether the blockchain is permissionedless or permissioned, who and what roles are the nodes, what is the consensus protocols) will deeply influence the interaction between the human actors and machines in the later stage, especially the evolve/crisis stage (Rikken et al., 2019). Thus, we believe that the strategic alliance research is still highly relevant, but it is vital to understand the novel governance of blockchain consortia in the decentralized age. Recent studies have explored the new governance model of blockchain, such as Rikken et al. (2019) and Tan et al. (2022) look at blockchain governance from a combination of algorithms and human lens; whereas Dursun and Üstünda (2021) lean toward the technical aspect and Van Pelt et al. (2021) anchor at the human side of blockchain governance.

Integrating the novel algorithmic governance into these nascent healthcare blockchain consortia entails a significant shift in governance paradigm which member leaders might not be fully aware of. The decentralization transfers not only decision-making but also information control—a vital asset of many organizations—beyond the boundaries of focal organizations. Unprepared for this might introduce the conflict between conventional perceptions of accountability (remains centralized) and decision-making ability (has become decentralized). Study in records and information management has illustrated this potential risk (Lemieux et al., 2020). Second, blockchain success requires the participants of several network participants, exemplified by the case of the IBM Food Trust (Goldsby & Hanisch, 2022), which has not been achieved by the majority of identified healthcare blockchain consortia. All in all, the sustainability of these blockchain consortia not

only depends on the effective management of the strategic alliances involved but also how these member organizations navigate the novel governance model of blockchain consortia.

5 Limitations of Research

Since our research question explored an emerging phenomenon, we believe our choice of unobtrusive archival data collection is the most suitable research approach as *"all of the unobtrusive strategies amount to examining and assessing human traces"* (Berg, 1954, p. 85). Having said that, we acknowledge two main limitations of our study design.

First, there is a risk of missing data. We minimized the chance of errors in data collection by deliberately tracking of our search history (i.e., exactly three pages of Google search results, noting the date of the search and any comments on each URL), constantly expanding and reviewing our search terms, and cross-checking with a paid data source. Via our informal discussion with the data vendor, we have learned that they also experienced the fragmented data of blockchain news in general and healthcare blockchain consortia in particular. Additionally, examination of the collected data occasionally identified inconsistent information. Despite these limitations, however, we believe that we have done the best possible things to achieve our research objectives.

Second, our study would have been richer with in-depth interviews with leaders of healthcare blockchain consortia. Absence of this data inhibited elucidating insights using a multi-case analysis technique. Even though the analysis of archival data returned novel findings that we presented, we were unable to explore the thoughts of industrial insiders and to provide a synthesis of their perspectives on healthcare blockchain consortia. We plan to conduct the second phase of this research employing an in-depth interview approach.

We hope this study can set a starting point for the discussion of healthcare blockchain consortia. This study showed that healthcare blockchain consortia seem to have a loose foundation of motives and management. Research to understand the characteristics of the novel blockchain consortia is strongly needed as described in the following.

6 Future Directions

As this study suggests, the majority of activities of healthcare in blockchain is establishing consortia; yet very little information is available regarding their motives, visions, and agenda for the consortia. Against the backdrop of traditional strategic alliances and emerging blockchain governance literature, a lot remains unknown in the arena of healthcare blockchain consortia. We suggest three future research streams that will have important theoretical and empirical implications.

First, there are many unexplored questions regarding what the optimal diversity of the consortia membership is. Blockchain is a team sport, which means it requires interorganizational collaboration to be effective (Tapscott & Tapscott, 2016; Vigna & Casey, 2015, 2018). Research in strategic alliances (Eklund & Kapoor, 2019) and blockchain consortia highlights the significance of diversifying membership. A recent study on the IBM Food Trust blockchain reinforced this idea, emphasizing the need to attract diverse industry participants for the blockchain's ultimate success (Goldsby & Hanisch, 2022).

Currently, a typical healthcare blockchain consortia involves only four industry sectors. The negotiating table seems lack of members across the healthcare value chain, including hospitals, clinics, health authorities, clinical labs, patient representatives (this one was not identified in the current consortia), technology, health product distribution, and universities to name a few. It is feasible to expect the expansion of healthcare blockchain consortia to non-healthcare organizations. The questions of who to be included and what value they can add remained to be explored.

The second point is closely related with the previous one, which poses question to the emerging concept of "blockchain ecosystem" mentioned in recent studies (Deloitte, 2019a; Goldsby & Hanisch, 2022). This concept has also been growing adopted in data management (Marcelo et al., 2019) and business (Aarikka-Stenroos & Ritala, 2017), but there is no definition of what an ecosystem in the blockchain context means. Comprehending the concept of a blockchain ecosystem and its defining characteristics is essential for both theoretical advancement and practical application of blockchain technology. This call for research in blockchain ecosystem resonates with Treiblmaier et al. (2021).

Third, interoperability has been and will be more important to healthcare blockchain consortia and healthcare blockchain consortia in general. Within the consortia identified in this paper, although Ethereum being a dominant protocol, there are various other options including Fabric, MultiChain, Quorum, and several unannounced protocols. Hence, the myriad of disparate consortia will likely perpetuate the problem of information and operational silos. This poses questions to research in cross-chain interoperability, information and data governance, and standards for data exchange to ensure the transparency, integrity, and security of data. To this end, we lack understanding in the information governance part of blockchain as the majority of research in blockchain governance focus on the challenges in blockchain governance from socio-technical perspectives (Lemieux, 2022). Interoperability is also identified as a growing area of interest in blockchain research (Treiblmaier et al., 2021).

7 Conclusions

Blockchain is expected to revolutionize healthcare as it increases security, auditability, and privacy of sensitive health data (Schumacher, 2018; Tapscott & Tapscott, 2017). Healthcare is also an active industry in experimenting with this novel

technology and most activities center around forming consortia. However, very little is known about these consortia, their members, visions, and use case. This study aims to explore the emergence of healthcare blockchain consortia to understand what these consortia are and the potential opportunities and challenges they have in light of interorganizational collaboration.

The study uses a qualitative, unobtrusive approach. We collected archival data from online public news websites for available healthcare blockchain consortia, their inception, members, and goals. Information about healthcare blockchain consortia is by and large fragmentary and unavailable. We were able to obtain a list of 19 healthcare blockchain consortia, most of whom are in established between 2017 and 2019 in the USA and EU. Most company join a single consortia, and half of the consortia had less than or equal to 5 members emphasizing the role of small consortia.

Notwithstanding the unstructured experimentation with this novel technology, the forming of consortia is supported by the strategic alliances literature for its benefits to reduce cost, increase legit and knowledge exchange, and booster problem-solving that any single organization shall be incapable of. However, reaping the benefits of these blockchain consortia is challenging as these consortia, by their publicly available information, seem not to crystalize their vision and objectives yet. The uncertainty and challenging of strategic alliances management is another significant obstacle for member organizations. In addition to that, blockchain consortia entails a novel form of governance, the collaboration between humans and algorithms, which adds another layer of uncertainty to the governance of these consortia.

We believe this study help reveal an underground part of blockchain consortia, which will be a useful starting point to a further and deeper discussion in this emerging phenomenon. Our findings may inform theorists and blockchain professionals of the distinctive behavior of blockchain consortia and facilitate future research in this emerging field. However, there remain many unexplored issues in the role of diversity of blockchain consortia membership, a definition and characteristics of blockchain ecosystem, standards for interoperability, and the role of information governance in blockchain consortia. These can be fruitful research areas which will have appreciable contribution theoretically and practically.

7.1 Key Terminology and Definitions (Optional)

If using unique terminology or definitions, consider adding this section. Here is an example of how to structure the information. As an example:

Participatory trial: A trial design refers to a structured approach in which a substantial number of volunteers, including both the general public and individuals whol self-identify with specific health conditions, can enroll themselves in a less formal study. This design is employed to assess the effectiveness of a particular approach in a real-world setting.

References

Aarikka-Stenroos, L., & Ritala, P. (2017). Network management in the era of ecosystems: Systematic review and management framework. *Industrial Marketing Management, 67*(September), 23–36. https://doi.org/10.1016/j.indmarman.2017.08.010

Banon, S. (2016). *The Tao of "The DAO" or: How the autonomous corporation is already here*. Retrieved from https://web.archive.org/web/20170706001536/https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/

Bass, J. (2019). *The seven major consortia (in chronological order)*. Retrieved December 17, 2019, from https://hashedhealth.com/consortia-july-2019-2/

Berg, B. L. (1954). *Qualitative research methods*. (K. Hanson, Ed.). Needham Heights: Allyn and bacon.

Bergquist, W., Betwee, J., & Meuel, D. (1995). *Building strategic relationships: How to extend your Organization's reach through partnerships, alliances and joint ventures*. (V. J. Carlton, Ed.). Jossey-Bass Inc. https://doi.org/10.1016/S0840-4704(10)60933-7

Bleeke, J., & Ernst, D. (1993). Collaborating to compete. In *Directors & Boards*. McKinsey & Co. Inc, John Wiley & Sons Inc.

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). *Blockchain beyond the hype: What is the strategic business value?* Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Clauson, K. (2019). *Personal post on LinkedIn*. Retrieved March 10, 2020, from https://www.linkedin.com/posts/kevinclauson_blockchain-consortia-initiatives-in-healthcare-activity-6578348079085338624-K2lC/

Deloitte. (2018). *Blockchain and the five vectors of progress*. Deloitte Insights.

Deloitte. (2019a). *Deloitte's 2019 global Blockchain survey: Blockchain gets down to business*. Deloitte Insights.

Deloitte. (2019b). *So, you've decided to join a blockchain consortia–Defining the benefits of 'coopetition.'*

Dursun, T., & Üstünda, B. B. (2021). A novel framework for policy based on-chain governance of blockchain networks. *Information Processing and Management, 58*(March), 102556. https://doi.org/10.1016/j.ipm.2021.102556

Duysters, G., Kok, G., & Vaandrager, M. (1999). Crafting successful strategic technology partnerships. *R&D Management, 29*(4), 343–351.

Eisenhardt, K. M., Graebner, M. E., & Sonenshein, S. (2016). Grand challenges and inductive methods : Rigor without rigor mortis. *Academy of Management Journal, 59*(4), 1113–1123.

Eklund, J., & Kapoor, R. (2019). Pursuing the new while sustaining the current: Incumbent strategies and firm value during the nascent period of industry change. *Organization Science, 30*(2), 383–404.

Goldsby, C., & Hanisch, M. (2022). The boon and bane of Blockchain: Getting the governance right. *California Management Review, 1*(28), 141. https://doi.org/10.1177/00081256221080747

Gomes-Casseres, B. (1993). *Managing international alliances: Conceptual framework*. Harvard Business School.

Gray, B. (1989). *Collaborating: Finding common ground for multiparty problems*. Jossey-Bass.

Gulati, R. (1995). Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of Management Journal, 38*(1), 85–112.

Huxham, C. (1996). *Creating collaborative advantage*. SAGE Publications.

Kale, P., & Singh, H. (2009). Managing strategic alliances: What do we know now, and where do we go from here ? *Academy of Management Journal, 23*, 45–63.

Kale, P., Singh, H., & Bell, J. (2009). Relating well: Building capabilities for sustaining alliance networks. In P. R. Kleindorfer, Y. Jerry, & R. Wind (Eds.), *Network challenge: Strategy, profit, and risk in an interlinked world (pp. 353–361)*. Wharton School Pub.

Kanter, R. M. (1994). Collaborative advantage: Successful partnerships manage the relationship, not just the deal. *Harvard Business Review*, 96–108.

Lei, D., & Slocum, J. W. J. (1991). Global strategic alliances: Payoffs and pitfalls. *Organizational Dynamics, 19*(3), 44–62.

Lemieux, V. L. (2022). *Searching for trust Blockchain Technology in an age of disinformation*. Cambridge University Press.

Lemieux, V. L., & Feng, C. (2021). *Conclusion: Theorizing from multidisciplinary perspectives on the design of Blockchain and distributed ledger systems* (part 2).

Lemieux, V. L., Hofman, D., Batista, D., & Joo, A. (2019). *Blockchain technology and record keeping*. Retrieved from http://armaedfoundation.org/wp-content/uploads/2019/06/AIEF-Research-Paper-Blockchain-Technology-Recordkeeping.pdf

Lemieux, V. L., Rowell, C., Seidel, M. L., & Woo, C. C. (2020). Caught in the middle? The era of blockchain and distributed trust. *Records Management Journal, 30*(3), 301–324. https://doi.org/10.1108/RMJ-09-2019-0048

Lewis, A. (2021). *The basics of bitcoins and blockchains: An introduction to cryptocurrencies and the technology that powers them*. Mango Publishing Group. https://doi.org/978-1-64250-673-0

Marcelo, M. I., de Barros Lima, G. F., & Farias Lóscio, B. (2019). *Investigations into data ecosystems: A systematic mapping study. Knowledge and information systems (Vol. 61)* (Vol. 61, p. 589). Springer. https://doi.org/10.1007/s10115-018-1323-6

Mattessich, P., & Monsey, B. (1992). *Collaboration: What makes it work*. A Review of Research Literature on Factors Influencing Successful Collaboration.

MediBloc. (2019). *MediBloc, Samsung, and SNU hospital selected by government for MyData Project*. Retrieved March 10, 2020, from https://medium.com/medibloc/ann-medibloc-samsung-and-snu-hospital-selected-by-government-for-mydata-project-5832de0a2f97

Merrill-sands, P. D., & Sheridan, B. (1996). *Developing and managing collaborative alliances: Lessons from a review of the literature*. Simmons Institute for Leadership and Change, Simmons College.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf

Ouchi, W. G. (1989). The new joint R&D. In *Proceedings of the IEEE* (pp. 1318–1326).

Van Pelt, R., Jansen, S., Baars, D., & Overbeek, S. (2021). Defining Blockchain governance: A framework for analysis and comparison. *Information Systems Management, 38*(1), 21–41. https://doi.org/10.1080/10580530.2020.1720046

PHBC. (n.d.). *PHBC*. Retrieved June 14, 2022, from https://www.phbconsortia.org/about.html

Porter, M. (Ed.). (1986). *Competition in global industries*. Harvard Business School Press.

Powell, W. W., Koput, K. W., & Smith-doerr, L. (1996). Interorganizational collaboration and the locus of innovation: Networks of learning in biotechnology. *Administrative Science Quarterly, 41*(1), 116–145.

Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organizations. *Information Polity: The International Journal of Government & Democracy in the Information Age, 24*, 397–417. https://doi.org/10.3233/IP-190154

Schumacher, A. (2018). Reinventing healthcare on the Blockchain toward a new era in precision medicine.

Seidel, M. L. (2017). Questioning centralized organizations in a time of distributed trust. *Journal of Management Inquiry, 27*(1), 40–44. https://doi.org/10.1177/1056492617734942

Siegel, D. (2016). *Understanding the DAO attack*. Retrieved March 10, 2022, from https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/

Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly, 39*(1), 101625. https://doi.org/10.1016/j.giq.2021.101625

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world*. Penguine Canada.

Tapscott, D., & Tapscott, A. (2017). Governance of the Internet's second era.
Treiblmaier, H., Swan, M., De Filippi, P., Lacity, M., Hardjono, T., & Kim, H. (2021). What's next in Blockchain research?–An identification of key topics using a multidisciplinary perspective. *The Data Base for Advances in Information Systems*.
Vigna, P., & Casey, M. J. (2015). *The age of cryptocurrency: How bitcoin and the blockchain are challenging the global economic order*. St Martin's Press.
Vigna, P., & Casey, M. J. (2018). *The truth machine: The blockchain and the future of everything*. St Martin's Press.
Walker, T. (2019). *Blockchain may save Billions for healthcare industry*. Retrieved March 10, 2020, from https://www.managedhealthcareexecutive.com/news/blockchain-may-save-billions-healthcare-industry

Trinh Nguyen-Phan, Ph.D. Student, School of Information, The University of British Columbia.

Trinh Nguyen is a second-year Ph.D. student at the School of Information at the University of British Columbia. Her research focuses on blockchain governance, blockchain in healthcare, and digital ecosystems. Trinh is a member of the Blockchain Graduate Pathway, a fellow of the Institute of Asian Research at the University of British Columbia, and has an educational and working background in business management and adult education, which explains for her interdisciplinary interests and approach in research.

Dr. Chang Lu is currently the cluster manager at Blockchain@UBC, the University of British Columbia, where he completed his postdoc research on blockchain adoption in healthcare. His theoretical research focuses on technology adoption, organization and institutional change, and the interplay between culture and power. He has published several articles on leading management journals and taught senior undergraduate and MBA students Organizational Strategy and Organizational Behavior. He serves as the supervisor of master and MBA students for their research projects, is currently creating education materials for executives about blockchain in healthcare. He earned his Ph.D. in Strategic Management and Organization, School of Business, from the University of Alberta. Prior to his academic career, he worked as an HR professional in China and Europe.