Metrics for Assessing Blockchain-based Healthcare Decentralized Apps

Peng Zhang, Michael Walker, Jules White, Douglas C. Schmidt
Vanderbilt University
Nashville, TN, USA
{peng.zhang, michael.a.walker.1, jules.white, d.schmidt}@vanderbilt.edu

Gunther Lenz
Varian Medical Systems
Palo Alto, CA, USA
gunther.lenz@varian.com

***Abstract*—Blockchain is a decentralized, trustless protocol that combines transparency, immutability, and consensus properties to enable secure, pseudo-anonymous transactions. Smart contracts are built atop a blockchain to support on-chain storage and enable Decentralized Apps (DApps) to interact with the blockchain programatically. Programmable blockchains have generated interest in the healthcare domain as a potential solution to resolve key challenges, such as gapped communications, inefficient clinical report delivery, and fragmented health records.**

This paper provides evaluation metrics to assess blockchain-based DApps in terms of their feasibility, intended capability, and compliance in the healthcare domain.

***Index Terms*—healthcare interoperability, blockchain, smart contracts, DApp, evaluation metrics**

I. Introduction

Blockchain is an unconventional platform that alleviates the reliance on a single, centralized authority, yet still supports secure and pseudo-anonymous transactions and agreements directly between interacting parties. It offers decentralization, immutability, and consensus via cryptography and game theory. Smart contracts are code built atop a blockchain that can be executed upon predefined conditions. They enable development of *Decentralized Apps* (DApps) to interact with blockchains and support on-chain storage [1].

In an interoperable healthcare environment, software apps and technology platforms, such as electronic medical records (EMRs), should be able to communicate seamlessly, exchange data, and use the exchanged data across health organizations and app vendors. They should also ensure effective care delivery for individuals and communities by allowing caregivers to collaborate within and beyond organizational boundaries [2]. Healthcare researchers and practitioners today, however, struggle with fragmented data, delayed communications, and gapped medical workflows caused by vendor-specific and incompatible health systems, making it hard to provide personalized care [3]. A fundamental problem is the lack of a trusted link that can connect these independent health systems together to establish an end-to-end reachable network (as shown in Figure 1).

Blockchain has emerged as a promising means to provide this trusted link due to its properties outlined above. As a result, various efforts [4], [5] have applied blockchains to improve healthcare interoperability. No studies have heretofore been published, however, to assess feasibility and verify the intended capability of these efforts. This paper presents our efforts to address this gap.

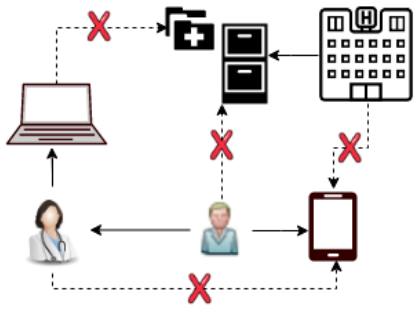

Fig. 1. Conventional Health Systems Do Not Connect Heterogeneous Data sources to Create an Interoperable Network

The remainder of this paper is organized as follows: Section 2 provides the context in which to evaluate DApps[1] for healthcare; Section 3 presents a set of evaluation metrics to assess healthcare DApps; Section 4 compares our work with research related to healthcare system assessments; and Section 5 presents concluding remarks.

II. Context and Current Limitations

This section provides background information and terminology in the context of healthcare interoperability to provide the foundation for Section III's metrics for evaluating blockchain-based healthcare DApps.

A. Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA privacy regulations [6] require the confidentiality and protection of individually identifiable health information that is transferred, received, handled, or shared by healthcare professionals and organizations. Moreover, only the minimum health information necessary to conduct business can be used or shared. All systems and apps created to share personally identifiable information(PII) must be HIPAA compliant. As a result, any PII accessed by the DApp or written to a public blockchain must be encrypted and securely managed by parties interacting with this app.

[1]All future references of DApps in this paper refer to blockchain-based healthcare apps

B. Definition of Healthcare Interoperability

Interoperability in healthcare allows two or more systems to exchange information and use the exchanged information [7]. The three levels of health information technology interoperability [8] ordered from lowest to highest fidelity are:

1) **Foundational interoperability** that enables data exchanges between healthcare systems without requiring the ability for the receiving party to interpret the data
2) **Structural interoperability** that defines the formats of exchanged clinical data and ensures that received data are preserved and can be interpretable at the data field using the predefined formats.
3) **Semantic interoperability** that allows for interpretation of data exchanged by not only syntax (structure) but also semantics (meaning) of the data.

The goal of defining this hierarchy of levels is to ensure that disparate health systems and device platforms deliver information with the requisite quality, safety, and cost-effectiveness. Foundational and structural interoperability are prerequisites for semantic interoperability, which is the hardest to achieve but highest in demand to improve quality of care. Unfortunately, without clinical domain knowledge or some standards that convey this knowledge, information systems cannot easily interpret myriad sources of health information.

Fast Healthcare Interoperability Resources (FHIR) [9] was created by the *Health Level Seven International* (HL7) organization as a draft standard API for describing the format of clinical data to exchange. FHIR increases the efficiency of information exchange processes by allowing the sharing of specific and well-defined pieces of information, rather than traditional document-centric approaches, which are overly broad and thus insecure. To move towards semantic interoperability, a modern healthcare app should support data schema standards like FHIR.

C. Modern Healthcare Model: Patient-Centered Care

Patient-centered care has become an emphasis in recent research and practice [10], [11]. In this model, patients have better access and control of their medical records to reduce information fragmentation and inaccuracy caused by communication delays or coordination errors [12]. Ideally, health apps should allow viewing of data in (near) real-time so that patients can be notified automatically as soon as medical documents are ready, *e.g.*, analyses are entered into the system. Conventional health systems, however, have several limitations that hinder the evolution to patient-centered model, as described in the remainder of this section.

1) Lack of Patient-controlled Access: Conventional health systems do not allow patients to easily modify or revoke a provider's access to their data. After a provider has a patient's data, therefore, they could possess it permanently. Morever, if a patient switches providers many times throughout their lifetime, many different providers will have their data, which increases the chance of data theft because it only takes one provider lacking security practices to put patient information at risk (assuming that no malpractice or malicious storing of patient data is involved). Alternately, a patient might want a different provider to access their medical data. With conventional health systems, however, there is no easy way to share the data or later revoke the second provider's access to it. The incompatibility of conventional health apps prevents the implementations of secure patient-oriented read/write access control mechanisms to solve these common issues.

2) Sporadic Support for Patient-Reported Outcomes (PROs): As PROs have become an integral part of patient health status [3], patients should be able to self-report their sickness symptoms. Currently, self-reporting capability is app-specific, meaning that patients can only access this feature if their provider's medical system implements it. With sporadic support of this feature in today's healthcare systems, it is hard to reflect PROs in patient health records.

III. Evaluation Metrics

Based on the healthcare domain context described in Section II, this section defines a set of evaluation metrics that can be used to assess DApps designed to address healthcare interoperability issues. Table I summarizes the metrics described below, which are ranked in the order of significance.

TABLE I
SUMMARY OF METRICS FOR EVALUATING DAPPS DESIGNED TO IMPROVE HEALTHCARE INTEROPERABILITY, ORDERED BY SIGNIFICANCE

	Assessment Metric
1	Entire workflow is HIPAA compliant
2	Framework employed needs to support Turing-complete operations
3	Support for user identification and authentication
4	Support for structural interoperability at minimum
5	Scalability across large populations of healthcare participants
6	Cost-effectiveness
7	Support of patient-centered care model

A. The Entire DApp Workflow Must be HIPAA Compliant

A core tenet of HIPPA compliance is that PII must be protected against a confidentiality breach. In particular, the end-to-end workflow of a healthcare app—from entering to processing then delivering the data—must be HIPAA compliant. Current health systems involving centralized data servers can encrypt and host data behind protected firewalls. When using a blockchain where all information is publicly available, however, it is non-trivial to securely manage and/or store sensitive data.

For example, storing encrypted health information on the blockchain is impractical for the following reasons:

- Significant storage cost and computational overhead would be inevitable to maintain and retrieve the data.
- Any data written into the blockchain will remain publicly available for the entire lifespan of that blockchain.

Moreover, if the encryption mechanism used to protect data on the blockchain is later broken, either by a new algorithm or by advances in computing power, the data would be vulnerable to attack. Even if encryptions strategies are regularly updated

to provide maximum reasonable protection, any temporary breach would result in serious consequences.

A well-designed healthcare DApp should limit the storage of encrypted sensitive data on the blockchain. For example, it may store some unidentifiable or encrypted metadata to refer to actual patient health information. Likewise, it may store only minimum resource required to obtain/exchange sensitive data through a trusted channel (such as a 3rd party Oraclize service [13]) that allows a contract on the blockchain to query/retrieve data sources outside the blockchain while ensuring they are genuine and untampered.

B. The Blockchain Platform Should Support Turing-Completeness

Many blockchain platforms are only used for a single purpose: *commodity exchanges*. For instance, Bitcoin [14] is designed as a cryptocurrency, *i.e.*, used to buy and sell commodities on a marketplace securely and pseudo-anonymously; and Litecoin [15] is used as digital cash for merchandising. Despite the popularity of these blockchain-based cryptocurrencies, they are not meant to exchange diversely-formatted data models, which are essential in the healthcare domain.

An interoperable health system should handle the exchanges of sensitive patient information. It should also facilitate communications amongst various parties. To design a modern healthcare app, therefore, the underlying blockchain platform should support Turing-complete operations, *i.e.*, it should contain programming features capable of solving any computation problem.

Ethereum [16] is an open-source blockchain platform with a smart contract feature that supports Turing-complete operations. It can thus be used for a wide (and open-ended) set of capabilities relevant for healthcare DApps, including health information sharing and data access control. Figure 2 is an example DApp we have developed using the Ethereum framework for managing patient data access control [17].

C. DApp Should Support User Identifiability and Authentication

Two types of participants require identification and authentication in healthcare: *patients* and *healthcare professionals* (*e.g.*, physicians, pharmacists, and other administrators, such as hospitals and insurance companies). These two groups are distinct because (1) there are *significantly* more patients than healthcare professionals and (2) healthcare professionals have easier access to health-related educative and training materials from their organizations. As a result, problems like forgetting or misplacing PII is more prevalent among patients.

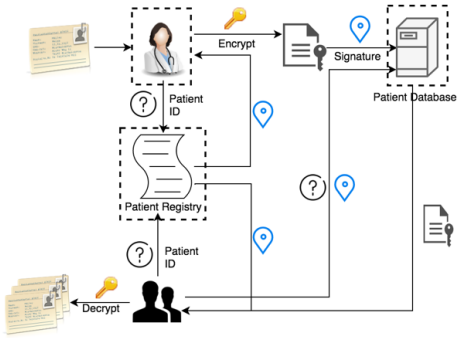

Fig. 2. An Example DApp Architecture Built on Ethereum

A good healthcare DApp should support user identifiability and authentication while providing strategies to mitigate lost PII. In particular, it should address various questions regarding organizational or individual user identification and authentication, such as (1) what information is needed to create a unique identifier that distinguishes each user while maintaining their anonymity on the blockchain, (2) how to convey new account information to users and allow them to access their accounts with unique identifiers, (3) how secure is the authentication technique employed, (4) will a user's authentication information be recoverable if lost or stolen, and (5) if an organization account is stolen, what impact will it have on users belonging to that organization?

D. DApp Should Support Structural Interoperability at Minimum

Semantic interoperability cannot be achieved by a DApp in isolation. Conventional health systems and apps have vendor-specific data models that must be upgraded or revamped to a unified design, which is a non-trivial process. For a DApp to provide minimum healthcare requirements, however, it should support at least structural interoperability (and ideally semantic interoperability), which enables the exchange of clinical data and interpretation of received data given the structures or formats implemented. To avoid introducing additional complexity caused by diverging data models used within the DApp, it should therefore respect and be able to work with popular data standards (such as FHIR described in II-B) as needed.

E. Scalability across Large Populations of Healthcare Participants

Since a production healthcare DApp may need to provide services for millions of users, it must be scalable. An important assessment of a DApp's feasibility is thus how it handles large amounts of traffic on the blockchain. For instance, if a DApp stores a registry of patients receiving care at a hospital, how much information can it manage to keep before the blockchain platform (such as Ethereum) terminates further operations from the app to prevent it from being a malicious attack?

As another example, a DApp may be used to bridge communication gaps across different care providers. In this case, how will it track and route activities to the appropriate participants among a large pool of users? A successful health app should leverage the blockchain to enhance interoperability, while maintaining its quality when users or components of the app scale up and out.

F. Cost-Effectiveness Compared to Existing Approaches

Network nodes/operators in typical blockchain deployments are rewarded with cryptocurrency as an incentive for their

contribution to maintain the decentralized ecosystem with data integrity and consensus. The incentive, however, comes with costs imposed on blockchain users with respect to storing information and performing computations.

In a healthcare DApp using these deployments, what will be the costs associated with the services and how will those costs compare with existing systems that are centralized and proprietary? Cost estimation is particularly important when a DApp provides services for *large* patient and provider populations. Likewise, if blockchain is used to replace certain components in the current medical systems to improve interoperability, is the new model more cost-effective than conventional solutions? Furthermore, what will be the cost of maintaining and upgrading the new system if/when necessary? Moreover, if operational costs are directly associated with the native cryptocurrency of the employed blockchain implementation, how will its fluctuation affect cost estimations?

G. Support of Patient-Centered Care Model

As healthcare shifts its focus towards the patient-centered care model discussed in Section II-C, blockchain-based health systems should grant patients easier access to—and control over—sharing their own medical data. Assessing this aspect of a DApp involves determining if it can overcome the limitations of conventional systems in providing patient-oriented features. These features may include health information self-reporting, access of personal medical records or prescription history from different providers, auditing existing accesses to patient health records, and the ability to share or revoke access to patients' own medical data.

IV. Related Work

Researchers have assessed existing healthcare systems and recognized the changes required to improve interoperability. For example, Kellermann et. al [18] analyzed existing systems in terms of their adoption, easy and effective use, and interoperability and described the necessary changes for improving these aspects. Similarly, Jones et. al [19] conducted a systematic review of health IT focusing on their quality, safety, efficiency, and effects of contextual and implementation. Cresswell et. al [20] identified key considerations during the technical lifecycle of large-scale health IT implementation and adoption for stages including establishing the need for change, system selection, implementation planning, and maintenance and evaluation.

Our research differs from prior work on assessing heath IT systems in several ways. First, we present a set of preliminary technical metrics especially targeting blockchain-based healthcare solutions. Second, we incorporate domain-specific healthcare requirements into the technical discussions so it is more relevant and apparent for healthcare researchers. In addition, these metrics can serve as a guide for future development using blockchain technologies.

V. Concluding Remarks

Blockchains offer properties of decentralization, transparency, and immutability that can potentially be leveraged to improve healthcare interoperability. Existing literature, however, provides little/no measures/guidelines for evaluating/creating blockchain-based healthcare apps. To bridge this gap, this paper described a set of evaluation metrics, from both the technical and domain perspectives, to assess healthcare DApps using this novel technology and serve as an initial guide for creating future apps in this domain. In future work, we will expand this research to explore other appropriate evaluation metrics and validate our findings using concrete blockchains-based healthcare use cases.

References

[1] D. Johnston, S. O. Yilmaz, J. Kandah, N. Bentenitis, F. Hashemi, R. Gross, S. Wilkinson, and S. Mason, "The general theory of decentralized applications, dapps," *GitHub, June*, vol. 9, 2014.

[2] ONC, "Connecting health and care for the nation: A 10-year vision to achieve an interoperable health it infrastructure," 2014.

[3] B. Middleton, M. Bloomrosen, M. A. Dente, B. Hashmat, R. Koppel, J. M. Overhage, T. H. Payne, S. T. Rosenbloom, C. Weaver, and J. Zhang, "Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from amia," *Journal of the American Medical Informatics Association*, vol. 20, no. e1, pp. e2–e8, 2013.

[4] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. IEEE, 2016, pp. 1–3.

[5] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:medrec prototype for electronic health records and medical research data," in *Proceedings of IEEE Open & Big Data Conference*, 2016.

[6] H. Office for Civil Rights, "Standards for privacy of individually identifiable health information. final rule." *Federal Register*, vol. 67, no. 157, p. 53181, 2002.

[7] A. Geraci, F. Katki, L. McMonegal, B. Meyer, J. Lane, P. Wilson, J. Radatz, M. Yee, H. Porteous, and F. Springsteel, *IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries*. IEEE Press, 1991.

[8] J. Lumpkin, S. P. Cohn, J. S. Blair *et al.*, "Uniform data standards for patient medical record information," *National Committee on Vital and Health Statistics*, vol. 53, 2003.

[9] HL7, "Fhir overview," 2014. [Online]. Available: https://www.hl7.org/fhir/overview.html

[10] J. Oates, W. W. Weston, and J. Jordan, "The impact of patient-centered care on outcomes," *Fam Pract*, vol. 49, pp. 796–804, 2000.

[11] A. Reynolds, "Patient-centered care," *Radiologic Technology*, vol. 81, no. 2, pp. 133–147, 2009.

[12] J. S. Ash, M. Berg, and E. Coiera, "Some unintended consequences of information technology in health care: the nature of patient care information system-related errors," *Journal of the American Medical Informatics Association*, vol. 11, no. 2, pp. 104–112, 2004.

[13] E. Foundation. (2015) Oraclize limited. [Online]. Available: http://www.oraclize.it/

[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *URL: http://www. bitcoin. org/bitcoin. pdf*, 2008.

[15] C. Lee, "Litecoin," 2011. [Online]. Available: https://litecoin.org/

[16] E. Foundation. (2015) Solidity. [Online]. Available: https://solidity.readthedocs.io/en/develop/

[17] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability in blockchain-based healthcare apps," *arXiv preprint arXiv:1706.03700*, 2017.

[18] A. L. Kellermann and S. S. Jones, "What it will take to achieve the as-yet-unfulfilled promises of health information technology," *Health affairs*, vol. 32, no. 1, pp. 63–68, 2013.

[19] S. S. Jones, R. S. Rudin, T. Perry, and P. G. Shekelle, "Health information technology: an updated systematic review with a focus on meaningful use," *Annals of internal medicine*, vol. 160, no. 1, pp. 48–54, 2014.

[20] K. M. Cresswell, D. W. Bates, and A. Sheikh, "Ten key considerations for the successful implementation and adoption of large-scale health information technology," *Journal of the American Medical Informatics Association*, vol. 20, no. e1, pp. e9–e13, 2013.