Computational and Structural Biotechnology Journal 16 (2018) 267–278

COMPUTATIONAL ANDSTRUCTURAL BIOTECHNOLOGY JOURNAL

journal homepage: www.elsevier.com/locate/csbj

# FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data

Peng Zhang [a,*], Jules White [a], Douglas C. Schmidt [a], Gunther Lenz [b], S. Trent Rosenbloom [c]

[a] *Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, USA*
[b] *Varian Medical Systems, Palo Alto, California, USA*
[c] *Department of Biomedical Informatics, Vanderbilt University Medical Center, Nashville, TN, USA*

ARTICLE INFO

*Article history:*
Received 26 April 2018
Received in revised form 16 July 2018
Accepted 21 July 2018
Available online 29 July 2018

*Keywords:*
Blockchain
Smart contracts
Decentralized app
Interoperability
Digital health identity
Clinical data sharing
Cancer care

ABSTRACT

Secure and scalable data sharing is essential for collaborative clinical decision making. Conventional clinical data efforts are often siloed, however, which creates barriers to efficient information exchange and impedes effective treatment decision made for patients. This paper provides four contributions to the study of applying blockchain technology to clinical data sharing in the context of technical requirements defined in the "Shared Nationwide Interoperability Roadmap" from the *Office of the National Coordinator for Health Information Technology* (ONC). First, we analyze the ONC requirements and their implications for blockchain-based systems. Second, we present FHIRChain, which is a blockchain-based architecture designed to meet ONC requirements by encapsulating the HL7 *Fast Healthcare Interoperability Resources* (FHIR) standard for shared clinical data. Third, we demonstrate a FHIRChain-based decentralized app using digital health identities to authenticate participants in a case study of collaborative decision making for remote cancer care. Fourth, we highlight key lessons learned from our case study.

## 1. Introduction

### 1.1. The Importance of Data Sharing in Collaborative Decision Making

Secure and scalable data sharing is essential to provide effective collaborative treatment and care decisions for patients. Patients visit many different care providers' offices during their lifetime. These providers should be able to exchange health information about their patients in a timely and privacy-sensitive manner to ensure they have the most up-to-date knowledge about patient health conditions.

As another example, in telemedicine practice Berman and Fenaughty [1]—where patients are remotely diagnosed and treated—the ability to exchange data securely and scalably is particularly important for enabling clinical communications regarding remote patient cases. Data sharing helps improve diagnostic accuracy Castaneda et al. [2] by gathering confirmations or recommendations from a group of medical experts, as well as preventing inadequacies Singh et al. [3] and errors in treatment plan and medication Kaushal et al. [4]; Schiff et al. [5]. Likewise, aggregated intelligence and insights Taichman et al. [6]; Warren [7]; Geifman et al. [8] helps clinicians understand patient needs and in turn apply more effective in-person and remote treatments.

Data sharing is also essential in cancer care, where groups of physicians with different specialties form tumor boards. These boards meet on a regular basis to analyze cancer cases, exchange knowledge, and collaboratively create effective treatment and care plans for each patient Gross [9]. Regional virtual tumor boards are also being implemented via telemedicine Ricke and Bartelink [10]; Marshall et al. [11] for institutions that lack inter-specialty cancer care due to limited oncology expertise and resources Levit et al. [12].

### 1.2. Administrative Support for Coordinating Health IT Efforts

The Office of the National Coordinator for Health Information Technology (ONC) is a division of the Office of the Secretary within the United States Department of Health and Human Services. ONC is the principal federal entity to oversee and coordinate health IT efforts, including the development of interoperable, privacy-preserving, and secure nationwide health information systems and the promotion of widespread, meaningful use of health IT to improve healthcare.

### 1.3. Data Sharing Barriers to Collaborative Decision Making

In practice, many barriers exist in the technical infrastructure of health IT systems today that impede the secure and scalable data sharing across institutions, thereby limiting support for collaborative clinical decision making. Examples of such barriers include the following:

* Corresponding author.
*E-mail addresses:* peng.zhang@vanderbilt.edu (P. Zhang), jules.white@vanderbilt.edu (J. White), d.schmidt@vanderbilt.edu (D.C. Schmidt), gunther.lenz@varian.com (G. Lenz), trent.rosenbloom@vanderbilt.edu (S.T. Rosenbloom).

https://doi.org/10.1016/j.csbj.2018.07.004

- Security and privacy concerns. Despite the need for data sharing, concerns remain regarding protection of patient identity and confidentiality Terry [13]. For instance, virtual medical interactions may increase the risk of clinical data breaches due to electronic transmission of data without highly secure infrastructures in place, which can result in severe financial and legal consequences Downey et al. [14]. Likewise, medical identity theft may occur more frequently, especially in telemedicine Terry [13], where virtual (i.e., networked) interactions are replacing face-to-face interactions between providers and patients.
- Lack of trust relationships between healthcare entities. Trust relationships between healthcare entities Hripcsak et al. [15] (e.g., care providers and/or healthcare institutions) are an important precondition to digital communications Hartvigsen et al. [16] and data sharing in the absence of custody over shared data. Larger healthcare facilities (such as enterprise hospital systems) may be networked Maheu et al. [17], but communications between private or smaller practices may not be established.
- Scalability concerns. Large-scale datasets may be hard to transmit electronically due to restrictive firewall settings or limitations in bandwidth (which is still common in rural areas LaRose et al. [18]). Lack of scalability can also impact overall system response time and data transaction speed Bondi [19].
- Lack of interoperable data standards enforcement. Without the enforcement of existing interoperable data standards (such as HL7's *Fast Healthcare Interoperability Resources* (FHIR)Bender and Sartipi [20] for shared data), health data can vary in formats and structures that are hard to interpret and integrate into other systems Richesson and Krischer [21].

What is needed, therefore, is a standards-based architecture that can integrate with existing health IT systems (and related mobile apps) to enable secure and scalable clinical data sharing for improving continuous, collaborative decision support.

Research focus and contributions → Architectural considerations for secure and scalable blockchain-based clinical data sharing systems. Blockchain technologies have recently been touted Das [22]; Mettler [23]; Azaria et al. [24] as a technical infrastructure to support clinical data sharing that promotes care coordination. A key property of blockchains is their support for "trustless disintermediation." This property enables multiple parties who do not fully trust each other to exchange digital assets (such as the Bitcoin cryptocurrency Nakamoto [25]), while still protecting their sensitive, personal data from each other.

Our prior work Zhang et al. [26] provided evaluation recommendations for blockchain-based health IT solutions on a high-level, focusing on common software patterns Zhang et al. [27] that can be applied to improve the design of blockchain-based health apps. This paper examines previously unexplored research topics related to alleviating the data sharing barriers described above, namely: *what are the architectural consideration associated with properly leveraging blockchain technologies to securely and scalably share healthcare data for improving collaborative clinical decision support*?

This paper provides the following contributions to using blockchain technologies in clinical data sharing to improve collaborative decision support:

- We summarize key technical requirements defined in the "Shared Nationwide Interoperability Roadmap" DeSalvo and Galvez [28] drafted by the *Office of the National Coordinator for Health Information Technology* (ONC) for creating an interoperable health IT system and analyze the implications for blockchain-based system design.
- We present the structure and funcationality of a blockchain-based architecture called FHIRChain that meets the ONC technical requirements for sharing clinical data between distributed providers. FHIRChain uses HL7's FHIR data elements (which have uniquely identifying tags) in conjunction with a token-based design to exchange data resources in a decentralized and verifiable manner without requiring duplicated efforts of uploading data to a centralized repository.
- We demonstrate a FHIRChain-based *decentralized app* (DApp) that uses digital health identities to more readily authenticate participants and manage data access authorizations in a case study of clinical data sharing in remote cancer care. This DApp enables users to share specific and structured pieces of information (rather than an entire document), thereby increasing the readability of data and flexibility of sharing options.
- We highlight key lessons learned from our case study and discuss how our FHIRChain-based DApp can be further extended to support other technical requirements for improving advanced healthcare interoperability issues, such as coordinating other stakeholders (e.g., insurance companies and pharmacies) across the industry and providing patients with direct and secure access to their own medical records. We also explore the data exchange issues that blockchains cannot yet address effectively, including semantic interoperability, healthcare malpractice, and unethical use of the data, which remain as future research problems in this space.

### 1.4. Paper Organization

The remainder of this paper is organized as follows: Section 2 provides an overview of blockchain technologies and the Ethereum platform, which is an open-source blockchain implementation that supports the development of DApps via "smart contracts;" Section 3 surveys different blockchain-based research approaches in the healthcare domain and compares our research on FHIRChain with related work; Section 4 summarizes ONC's key technical requirements for sharing clinical data and analyzes their implications for blockchain-based designs; Section 5 describes how the blockchain-based architecture of FHIRChain is designed to meet ONC requirements and motivates why we made certain architectural decisions; Section 6 analyzes the benefits and limitations of a case study that applied a FHIRChain-based DApp to provide collaborative clinical decision support; and Section 7 presents concluding remarks and outlines our key lessons learned and future work on extending the FHIRChain architecture described in this paper.

## 2. Overview of Blockchain

The most popular application of blockchain is the Bitcoin blockchain Nakamoto [25], which is a public distributed ledger designed to support financial transactions via the Bitcoin cryptocurrency. This blockchain operates in a peer-to-peer fashion with all transactions distributed to each network maintainer node (called a "miner") for verification and admittance onto the blockchain. These miners validate available transactions and group them into blocks, as shown in Fig. 1.

Miners then compete in solving a computationally expensive cryptographic puzzle, known as "proof-of-work," where a targeted hash value associated with the last valid block in the chain is calculated. The first miner to solve this puzzle receives a reward (i.e., an amount of Bitcoin) and appends their block of validated transactions to the blockchain sequence.

The Bitcoin blockchain uses the "proof-of-work" process outlined above to achieve consensus (agreement on the shared state and order of transactions) by

- incentivizing miners to contribute powerful hardware and electricity to the network with small amounts of cryptocurrency as rewards and
- discouraging rogue actors from attempting to manipulate or maliciously control the system.

After a block is added to the blockchain, its transaction history is secured from tampering via cryptography.