eHealthChain—a blockchain-based personal health information management system

Pravin Pawar[1] · Neeraj Parolia[2] · Sameer Shinde[3] · Thierry Oscar Edoh[4] · Madhusudan Singh[5]

Abstract

Medical IoT devices that use miniature sensors to collect patient's bio-signals and connected medical applications are playing a crucial role in providing pervasive and personalized healthcare. This technological improvement has also created opportunities for the better management of personal health information. The Personal Health Information Management System (PHIMS) supports activities such as acquisition, storage, organization, integration, and privacy-sensitive retrieval of consumer's health information. For usability and wide acceptance, the PHIMS should follow the design principles that guarantee privacy-aware health information sharing, individual information control, integration of information obtained from multiple medical IoT devices, health information security, and flexibility. Recently, blockchain technology has emerged as a lucrative option for the management of personal health information. In this paper, we propose eHealthChain—a blockchain-based PHIMS for managing health data originating from medical IoT devices and connected applications. The eHealthChain architecture consists of four layers, which are a blockchain layer for hosting a blockchain database, an IoT device layer for obtaining personal health data, an application layer for facilitating health data sharing, and an adapter layer, which interfaces the blockchain layer with an application layer. Compared to existing systems, eHealthChain provides complete control to the user in terms of personal health data acquisition, sharing, and self-management. We also present a detailed implementation of a Proof of Concept (PoC) prototype of eHealthChain system built using Hyperledger Fabric platform.

Keywords Blockchain technology · Hyperledger Fabric · Personal health information management systems · IoT integration · Adapter design pattern

✉ Madhusudan Singh
msingh@endicott.ac.kr

Pravin Pawar
pravin.pawar@sunykorea.ac.kr

Neeraj Parolia
nparolia@towson.edu

Sameer Shinde
sameer@softlabsgroup.com

Thierry Oscar Edoh
oscar.edoh@gmail.com

[1] Department of Computer Science, State University of New York, Korea, Incheon, South Korea

[2] Department of Business Analytics and Technology Management, Towson University, Baltimore, MD, USA

[3] Softlabs Technologies and Developments Pvt. Ltd., Mumbai, India

[4] Chair for Applied Software Engineering, Technical University of Munich, Munich, Germany

[5] Department of Technology Studies, Endicott College of International Studies, Daejeon, South Korea

1 Introduction

The healthcare industry is witnessing a transition from a traditional hospital-centric model to an individual-centric model that refers to an emerging trend of providing personalized services to the general population. The p-Health (Pervasive and Personalized Health) paradigm encourages the participation of the whole nation in the prevention of illnesses or early prediction of diseases [1]. Medical IoT devices and applications that use miniature sensors to collect patient's bio-signals and transmit data over low-cost wireless networks are playing a crucial role in achieving this vision.

There are a growing number of applications of Internet of Things (IoT) technologies in the healthcare industry. A wide range of IoT applications and devices are available for remote healthcare monitoring, consultation, and delivery. There are several medical IoT devices available in the consumer market for the measurement of bio-signals such as electrocardiogram (ECG), electroencephalogram (EEG),

blood pressure, respiration rate, heart rate, oxygen saturation (SpO2), body temperature, and blood glucose monitor [2]. Medical IoT devices can also provide functionalities such as medication intake using IoT-enabled pill bottle [3], monitor inhalation flow rate and volume using smart inhaler [4], and regulate the working insulin infusion pump [5]. There are also several IoT devices available for the measurement of physical activity, sleep, and weight. As these devices are getting popular in the mainstream, the individuals are becoming the producer of health data. This is complimentary to conventional system where the health data originates from the hospitals. Furthermore, the COVID-19 pandemic has accelerated the adoption of remote health monitoring globally, and thus, the individuals are increasingly becoming responsible for the self-management of their health that includes activities such as regular monitoring and recording of health data and sharing this data with the caregivers and healthcare professionals as needed.

The personal health information could be divided into several types such as contacts of healthcare professionals, appointment calendar, patient diary, symptoms, prescriptions, surveys, medication logs, medical bills and receipts, diagnosis information, family history, x-ray and lab test medical records, and insurance information. A survey of consumers' perspectives on personal health information management reported in [6] suggested that individuals would like to have control over their personal health information; however, it is fine to share information necessary for quality care with the clinician. However, there are certain considerations in sharing and managing personal health data. The data originating from medical IoT devices is privacy-sensitive in nature, and legal regulations such as HIPAA regulations need to be enforced while disclosing the data to authorized parties. The Health Insurance Portability & Accountability Act (HIPAA) privacy regulations require health care providers and organizations, as well as their business associates, to develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared in the paper, oral, or electronic forms [7].

These considerations have led to the rise of Personal Health Information Management System (PHIMS) that supports activities such as acquisition, storage, organization, integration, and privacy-sensitive retrieval of consumer's health information, thus facilitating compliance with existing privacy laws [7, 8]. Recent technological advances have seen the rise of blockchain technology and its multiple compelling features such as chronological and time-stamped data record, auditable and cryptographically sealed information blocks, consensus-based transactions, policy-based access to facilitate data protection, fault-tolerant, and distributed ledger [9]. Blockchains connect stakeholders directly without requirements for third-party brokers; they are cost-effective and distributed ledgers providing increased accessibility to information [10]. Due to these features, blockchain technologies are a lucrative option for PHIMS implementation. We have presented a brief survey of using blockchain technology for the management of health data in Sect. 2.

Figure 1 shows an extended scenario of using blockchain technology for health information management where multiple information records such as mobile health care, medical insurance information, family health record, doctor's prescription, medication history, as well as genomic medical insurance claims can be stored in a blockchain server on cloud and can be accessed from the authorized persons (such as doctors/patients/researchers) based on patient's consent.

In this paper, we present eHealthChain, which is a Blockchain technology-based personal health information

Fig. 1 Blockchain-enabled health information
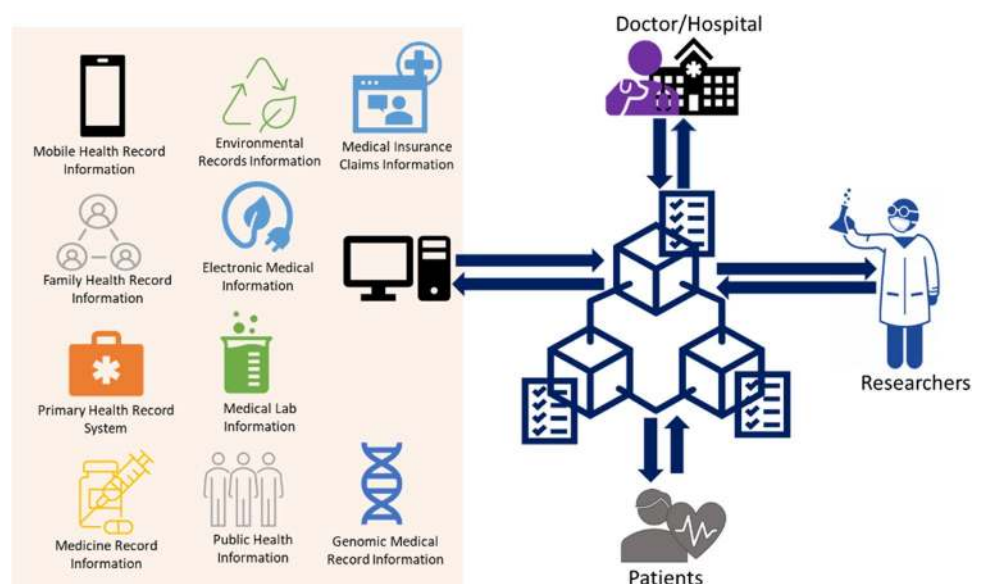
management platform for the acquisition, management, and sharing of personal health information obtained from medical IoT devices. The eHealthChain system interfaces medical IoT devices with the blockchain storage using a custom-designed adapter component. The adapter component is responsible for collecting data from IoT devices and storing data in the blockchain. Adapter component is also responsible for the retrieval of data from blockchain store and sends it to the application, which provides a user-friendly view of stored data.

The remainder of this chapter is organized as follows: Sect. 2 of this paper discusses related work. Section 3 presents ethical and legal considerations as well as outlines requirements for a blockchain-based personal health information management system. Section 4 elaborates the architecture of proposed eHealthChain platform and discusses its features. Section 5 discusses Hyperledger Fabric-based implementation of eHealthChain. Section 6 concludes the paper and provides directions for future work.

2 Related work

The PHIMS has become one of the critical factors of the demand for the increasing amount of processing power, developments in personal area network technologies, and advances in medical sensing; mobile devices are turning into the producer of personal health data. Several approaches have been proposed for managing data originating from personal health devices. Martíez et al. [11] propose a system architecture and provide implementation for the interoperability and end-to-end communication between personal health devices following the ISO/IEEE11073 standard and electronic health records following the ISO/EN13606 standard. Lee et al. [12] propose an intelligent service model for healthcare on top of data measurement and storage functionality provided by IoT health devices. To obtain data from personal health devices, an application level collaboration protocol is proposed in [12] which receives bio-signals information from the IoT-enabled devices. Rajput et al. [13] propose an IoT-based architecture to obtain health-related data from sensors and upload it to the cloud database for sharing with clinicians. Zgheib et al. [14] present a new IoT architecture for healthcare applications with a focus on the principles of weak coupling and of semantic data exchange.

Gaggioli et al. present in [15] a data collection platform named Psychlog which collects users' psychological, physiological, and activity information for mental health research. This application collects self-report questionnaires as well as heart rate and activity data using wireless ECG sensor and accelerometer, respectively. It combines data from self-reports and sensors to investigate relationship between psychological and physiological variables. In [16], Adjerid et al.

present the benefits of data exchange across organizations. They clearly pointed out that health information exchanges through electronic health records systems are more efficient.

As such, many (open source) implementations of health information systems already exist. A survey of open source health information systems [17] reports systems such as ClearHealth, Caisis, OpenMRS (Open Medical Record System), VistA (Veterans Health Information Systems and Technology Architecture), WorldVistA (an improved version of VistA), and OSCAR (Open Source Clinical Application Resource), OpenEMR and Tolven. A complete personal health record system named Indivo is also described. Indivo is a three tier-system with Indivo API that allows the system to collect health records from various sources and share these records with third parties in a privacy-sensitive manner.

Engelhardt [11] introduces blockchain technology in the healthcare sector. Accordingly, blockchain technology is best suited for the storage and sharing of health information because of the following reasons:

- Healthcare sector is composed of multiple stakeholders (such as patients, doctors, caregivers, and pharmacists).
- More trust is required between stakeholders than currently exists.
- Trust or efficiency increases in the absence of any intermediary.
- Reliable tracking of health bio-signals is required.
- For further analysis, bio-signal data need to be reliable over time.

In [18], Siyal et al. discuss the application of blockchain technology in medicine and healthcare domain. The article claims that blockchain technology has a potential to help in personalized, authentic, and secure healthcare by merging the entire real-time clinical data of a patient's health and presenting it in an up-to-date secure healthcare setup. However, they mentioned issues relating to data emanating from diverse sources and pointed out the interoperability issues between blockchains from various service providers.

MedRec is one of the first blockchain-based platforms for managing health data proposed by Azaria et al. [19] in which the health record data is provided by doctors. MedRec is prototyped on top of Ethereum blockchain [20]. MediBchain proposed by Al. Omar et al. [21] is another patient-centric healthcare data management system that uses blockchain as storage to attain privacy. In [21], the details of the protocol to ensure privacy are given; however, no implementation is discussed.

The Hyperledger Fabric blockchain network has been used for tamper-resistant storage of medical data by Ichikawa et al. [22]. They developed a mHealth system for cognitive behavioral therapy for insomnia using a smartphone

app whereas data collected with the app were stored in JavaScript Object Notation (JSON) format and sent to the blockchain network. In [23], Zhang et al. introduce the use HL7 Fast Healthcare Interoperability Resources (FHIR) on top of Ethereum Blockchain to securely exchange health information among institutions. The study has been named as FHIRChain and it shows how combining FHIR and block-chain technology can assure interoperable and secure data exchange in a case study of collaborative decision making for remote cancer care.

Since the proposed PHIMS has integrated concepts from mobile device, blockchain theory, and machine learning, it is a powerful eHealthChain management model for the PHIMS. The main challenges of blockchain-based system are the size of each transaction. Therefore, the proposed eHealthChain system is that the individual's health data is collected from multiple medical IoT devices which is available to the consumers, and this information is made available to the patient and clinicians in a secure and privacy-sensitive manner. In the eHealthChain system, instead of the hospital, an individual is the provider of data and is responsible for the management of own health record.

3 Considerations for personal health information management system

As the number of consumer Health IoT devices grow, the organizational, ethical, and economic challenges grow in proportion. In this section, we present our perspectives on various considerations for the blockchain-based PHIMS followed by high-level requirements for such a system.

3.1 Organizational, ethical, and economic considerations for blockchain-based PHIMS

With the growth in the amount of IoT devices and corresponding data, there is an emergence of an online business called data brokers or information brokers which store, analyze, and sell this data or third-party businesses. Examples of data brokers in North America include Acxiom, DataLogix, Experian, Ameridex, and Equifax. Third-party businesses use this data to target identifiable users to push advertising, recommendations, and service customization. Users are not explicity informed about how their data is stored, analyzed, and utilized as privacy-related terms and conditions are hidden inside lengthy terms and contracts. Furthermore, several data brokers such as Equifax, Exactis, and Choicepoint have suffered security breaches resulting in tremendous loss to consumers.

With a PHIMS running on blockchain, users can gain control over their personal data and enabling them to transact with other parties without the need for a data broker.

For example, the Eastman Kodak company has created KODAKOne, a blockchain-based platform for digital photography with its own currency, called KodakCoin which will allow photographers to own rights to images and get paid for licensing their content. The decentralized Brave Browser offers a blockchain-based rewards system aimed at changing the relationship between users, advertisers, and content creators. The Brave browser is a privacy-centered open-source blockchain-based browser that blocks ads and website trackers. Users of the browser receive a percentage of the advertising revenue share as a reward for their attention in the form of the browser's native cryptocurrency. The browser claims that the advertisements displayed to the users are aligned with their preferences, removing expenses and risks about privacy, security, and fraud. Building on these examples, we believe that users would be interested in monetizing their PIMS data with businesses like insurance providers which could provide discounts on health care premiums or products and services subject to privacy, transparency, and security controls. Previous research has provided several monetization models involving different stakeholders and marketplaces [24–26]. Several studies have proposed blockchain-based monetization solutions for IoT data [27, 28].

Presently, user's health data obtained from medical IoT devices is stored in cloud-based databases which are owned by the device manufacturers. Specialized medical device manufacturers such as Omron would be interested in building blockchain-based PHIMS applications for data collection. Popular wearable consumer product companies such as Apple and Google can be expected to provide PHIMS features in their existing or new mobile apps such as Apple Health, Google Fit and extend their backend storage with blockchain technology.

We can expect standalone blockchain-based PHIMS applications to be offered as a cloud-based service to the end users similar to Drop Box, Google Drive, and various anti-virus applications. There could be several factors which could support adoption. Medical IoT manufacturers may integrate blockchain in their PHIMS apps as a differentianing attribute or demonstrate their emphasis towards privacy. Conversely, blockchain-based PIMS could increase overall product costs and reduce opportunities for monetization of user data.

The COVID-19 pandemic has accelerated the adoption of remote telehealth and monitoring globally. Issues such as privacy and security would increase impetus for integrating blockchain technology in patient centered health care delivery models. As the amount of data increases in the PHIMS, we would expect a corresponding increase in attention to the analytics value of this data from different stakeholders. Legal and ethical issues could arise pertaining to ownership and access

to the data among various stakeholders besides the user such as the private block chain provider, PHIMS developer, insurance, and public/private health care providers.

3.2 High-level requirements for the blockchain-based PHIMS

The following points are the high-level requirements for a blockchain-based PHIMS:

- Support for personal health devices being sold by multiple manufacturers and which provide functionality to measure a variety of bio-signals;
- Capability to add or remove personal health devices as required;
- Should be able to function even though one or more personal health devices are offline;
- Ability to create uniform personalized health data record by acquiring data from multiple devices;
- Automatic confirmation of each new addition in a data record;
- Maintaining a permanent chronological history of data record updates;
- Provide user-friendly interface/dashboard of person's health data;
- Ability to provide data to third-party systems (such as a clinician, caregiver) based on user consent so that health data can be used for analysis and diagnosis purposes;
- Protect database from unauthorized access; and
- Verification and confirmation of each data record without the need of central regulatory authorities or a central database server.

4 eHealthChain architecture details

There are several medical IoT devices and applications available in the consumer market. These devices have a corresponding mobile app, which connects to the device, obtains health data, and sends device data to the backend for storage. The eHealthChain architecture consists of an adapter component that collects data from device backend store and transfers it to the blockchain for storage. The adapter component is also responsible for retrieving data from the blockchain and sends it to the application, which provides a user-friendly view of stored data. The use of adapter components is motivated by the adapter software architecture pattern, which allows reusability of existing functionality. The architecture of eHealthChain consists of four primary layers as shown in Fig. 2.

4.1 Blockchain layer

The blockchain layer provides functionality to implement and host a blockchain database. The health information obtained from medical IoT devices is stored in a blockchain database. Access to this data is provided only to authorized entities based on the consent of health data owner. The existing blockchain platforms could be broadly categorized into two types: public blockchain and private blockchain. The differentiating factor here is whether a blockchain is open for joining and participating in the network. In a public blockchain like the bitcoin blockchain, any entity can join and participate as well as view the ledger, blocks, and record data inside the blocks. In contrast, private blockchains also called "Permissioned blockchain" grant specific rights and restrictions to participants in the network who are required to obtain an invitation or permission to join [29]. Private

Fig. 2 Layered architecture of the eHealthChain system
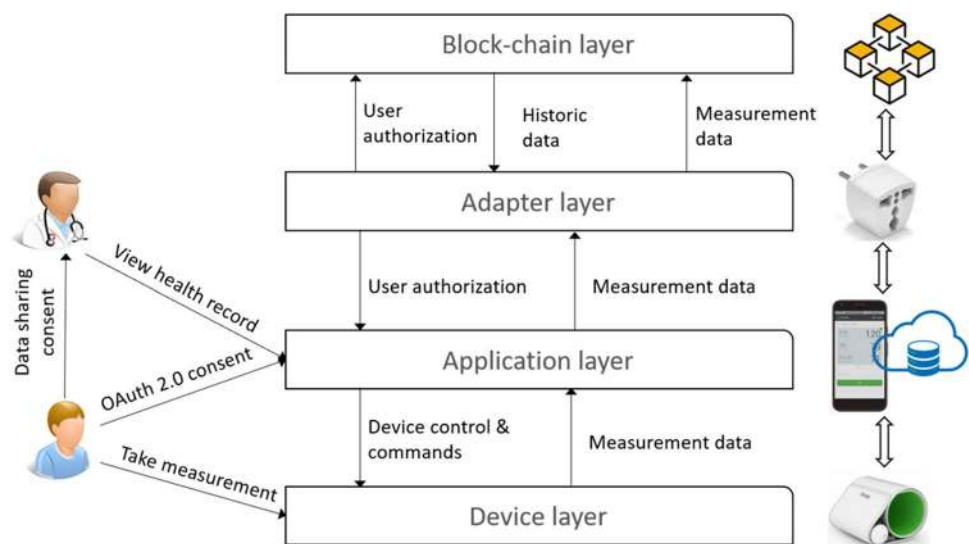
blockchains are more suitable for the implementation of PHIMS as they allow only authorized entities to join the blockchain network.

4.2 Adapter layer

The adapter layer has a responsibility of interfacing application layer with the blockchain layer. The adapter layer essentially works as a client of REST APIs provided by the blockchain layer and a client of services provided by an application layer. The adapter layer obtains user's health data using OAuth 2.0 protocol that ensures user's consent. After obtaining user's health data, the adapter layer uses REST APIs provided by the blockchain layer to write health data to the blockchain. In addition, the adapter layer works as a participant in the blockchain business network to obtain health data using REST API. The adapter layer may also provide this data to a dashboard application in the application layer which allows users to view consolidated health data.

4.3 Application layer

The entities at the application layer consists of mobile applications which collect data from consumer health devices, applications which function as health data sources and applications which allow users and clinicians to see consolidated health data obtained from the blockchain layer. Usually, health devices have corresponding mobile apps, which allow the management of specific health data. This data is also stored regularly in the application backend, possibly in the cloud database and is accessible using proper user credentials, e.g., Fitbit app tracks parameters such as user activity, exercise, food, weight and stores this data in the Fitbit store. Google Fit app records user activity using inbuilt mobile device accelerometer and stores this data as well as data originating from several supported devices such as Strava running and cycle tracking app, Polar Balance weighing scale, and Wear OS smartwatch in Google store. Usually, these apps allow sharing device data to external parties using OAuth 2.0 protocol. OAuth 2.0 is an authorization framework that enables third-party applications to obtain limited access to user accounts based on user consent.

4.4 Device layer

The device layer consists of medical IoT devices such as health watch, activity trackers, weighing scale, and smart pill bottles. These devices are IoT-enabled, capable of connecting to handheld mobile devices using short-range wireless technologies such as Bluetooth and function as data sources, which collect data specific to a person or entity such as home or place. A consumer generally operates these devices via a corresponding mobile app.

handheld mobiles also function as health data devices if corresponding applications are installed.

In the eHealthChain system, a patient is in charge of updating personal health information and is able to access the information using direct authorization. Patient has the authority to verify other stakeholders such as clinician/nurse/caregiver who has access to patient's data and vice versa. Since the PHIMS is based on blockchain technology, the stored data can be accessed using a mutual verification. As shown in Fig. 2, a patient provides consent to the application layer for obtaining health data from the IoT devices backend and provides data sharing consent to the doctor.

5 Leveraging Hyperledger fabric platform for building the eHealthChain system

In this section, we introduce some key concepts in a blockchain network as well as Hyperledger Fabric platform that is our choice for building the eHealthChain system.

5.1 Key concepts in a blockchain network

A blockchain network is composed of multiple peer-to-peer computing nodes. In a blockchain network, a distributed ledger maintains a record of all transactions that are executed in the network. A blockchain ledger is decentralized as it is replicated across the participants of the network collaborating in the maintenance. The information can only be appended in the blockchain using cryptographic techniques, which guarantee the immutability of the record. A smart contract provides controlled access to the ledger and allows participants to control and execute certain aspects of transactions according to the terms of an agreement. A smart contract can be coded according to the terms agreed by the parties involved in the record and subsequent actions can be initiated depending on the agreement.

Consensus refers to the process of approving and synchronizing ledger record across the network. In the traditional system, the members of a business network transact with each other while maintaining sperate records. In comparison, in a blockchain network, every participant has own copy of the ledger, which is replicated with other participants, and the consistency of this record is ensured using consensus mechanisms. A blockchain network shares the ledger information as well as the processes to update the ledger. In comparison to the traditional business network, blockchain networks reduce the risk, cost, and time in sharing private information and improve visibility and trust among the network participants.

5.2 Key concepts of Hyperledger Fabric

The frameworks such as Ethereum, HydraChain, Hyperledger Fabric, and MultiChain facilitate developing blockchain applications. Ethereum is one of the popular public blockchain platforms while HydraChain extends the Ethereum platform by supporting creation of permissioned blockchain [30]. Hyperledger Fabric [31], Multichain [32] are examples of private blockchain platforms. The smart contracts in Hyperledger Fabric [31] are called "chaincode" and they comprise the application logic of the system. The external applications can use blockchain smart contracts using REST APIs that are exposed by the Hyperledger Fabric and Ethereum platforms.

Hyperledger fabric is a project by Linux Foundation initiates in 2015 to advance cross-industry blockchain technologies using a collaborative community process-based approach. It is a private and permissioned blockchain which does not require protocols like "proof of work" to validate transactions record. The members of Hyperledger Fabric network use a trusted Membership Service Provider for enrolling in the network [33]. A shared ledger in Hyperledger Fabric consists of two components. The world state component is a database of the ledger, which describes the state of the ledger at any given point in time. The second component is record log component which keeps a record of all transactions leading to the current world state. Assets are the objects, which are to be maintained on the ledger.

A smart contract in Hyperledger Fabric is written in chaincode (which can be implemented using Go and Node languages) and it is invoked by an external application when interaction is required with the ledger. Chaincode record is used to modify assets. A Hyperledger Network uses a channel over which the business network participants communicate for ensuring privacy. Each channel consists of its own ledger and each peer in the channel maintains a copy of the ledger. A Hyperledger Fabric ledger supports operations such as query and update ledger. A query represents chaincode invocation that reads the current state of the ledger, but does not write to the ledger.

Hyperledger Fabric allows network participants to choose a consensus mechanism such as crash fault-tolerant (CFT) or byzantine fault-tolerant (BFT) ordering. This is a different process than Bitcoin, which uses mining technique that consists of solving a cryptographic puzzle to determine the node who publishes a block consisting of several record. A Hyperledger Fabric channel is a private "subnet" of communication between two or more specific network members, for the purpose of conducting private and confidential record. A channel consists of its own ledger shared across the entire network. However, a ledger can be privatized to include only a specific set of participants by creating another separate channel and isolating their ledger and record.

Members (organizations), anchor peers per member, the shared ledger, chaincode application, and the ordering service node define a channel. A member is a legally separate entity that participates in the network. An anchor peer is a node that is discoverable and communicable by other peers. Every participating organization (member) in a channel has an anchor peer [34]. A chaincode application is a software, which runs on a ledger to encode assets and executes the transaction instructions that contains business logic for modifying the assets. Ordering service nodes are responsible for ensuring order of records into a block. The transactions are ordered on a first-come-first-serve basis. A Membership Services Provider (MSP) is an abstract component of the system, which is responsible for providing credentials to clients and peers to participate in a network. These credentials are used for authenticating record and record processing results.

Each record on the network is executed on a channel, where each party must be authenticated and authorized to transact on that channel. Each peer that joins a channel has its own identity given by an MSP, which authenticates each peer to its channel peers and services [32]. A consortium of multiple

Fig. 3 Application use-case of eHealthChain system, which uses Hyperledger Fabric as a blockchain platform
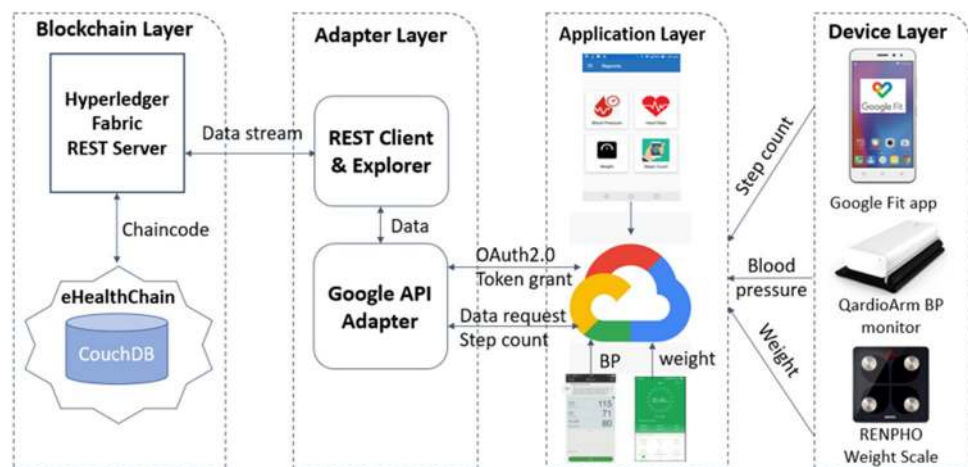
Fig. 4 eHealthChain blockchain network topology.
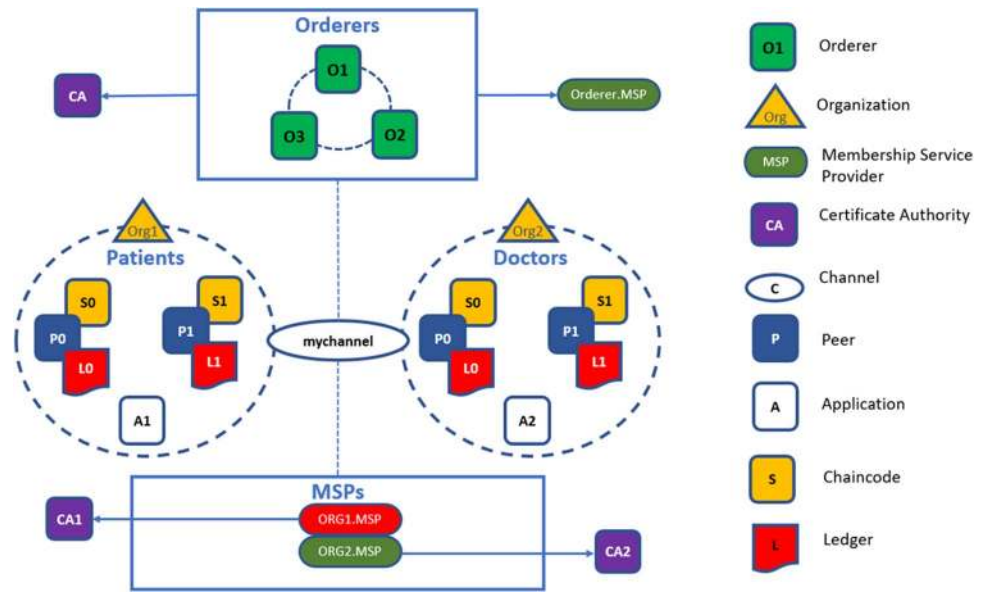
organizations forms a network and there are associated set of policies agreed by the consortium when the network is originally configured [35]. Subject to the agreement of the organization, network policies may change over the period.

5.3 Application use-case of eHealthChain system

Figure 3 shows an application use-case of eHealthChain system, which uses Hyperledger Fabric as a blockchain platform. We have implemented this use-case and have elaborated its detailed implementation in Sect. 6. In this case, the components of the device layer are two medical IoT devices and Google Fit application. The IoT devices are QardioCore blood pressure monitor and RENPHO digital weighing scale, which are available for purchase online. The application layer corresponds to eHealthChain mobile application and backend cloud stores provided by IoT device manufacturers [36]. The adapter layer consists of programmed components to perform OAuth 2.0 based authentication with the cloud store Google Fit and fetch data for storage in the Hyperledger Fabric blockchain. The components at the adapter layer are also responsible for fetching health data assets from the Hyperledger data store. This data is used at the application layer by the eHealthChain mobile app, which provides consolidated view of health data as per patient consent.

6 eHealthChain implementation details

In this section, we present eHealthChain implementation details that include blockchain network topology, brief description of chaincode, and details about developed mobile application with respect to implemented use-case.

6.1 eHealthChain blockchain network topology

Figure 4 shows the topology of the eHealthChain blockchain network. The infrastructure part of the eHealthChain network comes with two organizations, Org1 for patients and Org2 for doctors, each with two peer nodes (peer0 and peer1). Hence, in the eHealthChain network, there are four peer nodes in total. Each peer node runs a couchDB as a world state database. Each of the Org1 and Org2 has a corresponding Certificate Authority (CA) running fabric-CA software with proper configuration. The organizations also have corresponding Membership Service Providers (MSPs). There is an orderer organization with three orderer nodes. The orderer organization also has corresponding MSP and CA. All components are deployed as docker containers running on a host machine.

```
type Patient struct {
    PatientName    string `json:"patientname"`
    Gender   string `json:"gender"`
    Address  string `json:"address"`
    Phone    string `json:"phone"`
}

type PatientRecord struct {
    UserId     string `json:"userid"`
    RecordDate     string `json:"recorddate"`
    PatientRecordData   string `json:"patientrecorddata"`
}

type DataShareRequest struct {
    From    string `json:"from"`
    To    string `json:"to"`
    EndDate   string `json:"enddate"`
}
```

Fig. 5 *Patient*, *PatientRecord*, and *DataShareRequest* data structures

Fig. 6 Init function

```
// Init ;  Method for initializing smart contract
func (s *SmartContract) Init(APIstub shim.ChaincodeStubInterface) sc.Response {
    return shim.Success(nil)
}
```

6.2 Understanding eHealthChain chaincode

The eHealthChain chaincode is executed on the peer nodes inside a blockchain network. The business logic resides in the chaincode. The ledger is updated whenever the chaincode is invoked. The eHealthChain chaincode is written in Go language and it follows a specific pattern as per the requirements of Hyperledger Fabric. In this section, we only focus on important portions, which are the data structure, the *Init()* and *Invoke()* functions and some other functions which will be called by *Invoke()*.

6.2.1 Data structures

The eHealthChain data structures consist of three primary structures. The *Patient* structure represents basic information about the patient. The *PatientRecord* structure holds patient's health record data. The JSON format used is flexible to accommodate a variety of health data types. The request for sharing health record data is represented by the *DataShareRequest* structure (Fig. 5).

6.2.2 Init() and initLedger() functions

The *Init()* function is executed on the instantiation of chaincode in the Hyperledger Fabric network. The *Init()* function can be used to set as many initial states as possible. As a good practice, we leave this function empty and the *initLedger()* function is invoked externally. The *initLedger*

function preloads two sets of dummy patient data into the ledger using *PutState()* API. This function is executed only once (Figs. 6 and 7).

6.2.3 Invoke() function

The *Invoke()* function defines the actions using functions when the client application invokes the chaincode (Fig. 8). The argument list provided while invoking the chaincode includes the function name to be executed and arguments list for that function. The functions which will be executed are the following: *initLedger()*, *createPatient()*, *createPatientRecord()*, *queryRecord()*, *queryRecordByDate()*, *createDataShareRequest()*, and *queryDataShareByTo()*. These functions are also briefly explained in this section.

The *createPatient()* function creates a patient in the ledger. The data required for this function is given as a part of the Patient structure.

The *createPatientRecord()* function creates a patient health data record in the ledger. The data required for this function is given as a part of the PatientRecord structure.

The *queryRecord()* function allows query on an individual patient record based on *UserId*.

The *queryRecordByDate()* function allows query on an individual patient record based on *UserId* and a particular date.

The *createDataShareRequest()* function creates a request from a patient to doctor for viewing the patient record. The request has an end date, after which the request expires.

```
func (s *SmartContract) initLedger(APIstub shim.ChaincodeStubInterface) sc.Response {
    patients := []Patient{
            Patient{PatientName: "user1",Gender: "male",Address: "address1",Phone: "1234567890"},
            Patient{PatientName: "user2",Gender: "male",Address: "address2",Phone: "1234567890"},
        }
    i := 0
    for i < len(patients) {
        patientsBytes, _ := json.Marshal(patients[i])
        APIstub.PutState("PATIENT"+strconv.Itoa(i), patientsBytes)
        i = i + 1
    }
    return shim.Success(nil)
}
```

Fig. 7 initLedger function.

Fig. 8 Invoke() function

```
// Invoke :  Method for INVOKING smart contract
func (s *SmartContract) Invoke(APIstub shim.ChaincodeStubInterface) sc.Response {

    function, args := APIstub.GetFunctionAndParameters()
    logger.Infof("Function name is:  %d", function)
    logger.Infof("Args length is : %d", len(args))

    switch function {
    case "initLedger":
        return s.initLedger(APIstub)
    case "createPatient":
        return s.createPatient(APIstub, args)
    case "createPatientRecord":
        return s.createPatientRecord(APIstub, args)
    case "queryRecord":
        return s.queryRecord(APIstub, args)
    case "queryRecordByDate":
        return s.queryRecordByDate(APIstub, args)
    case "createDataShareRequest":
        return s.createDataShareRequest(APIstub, args)
    case "queryDataShareByTo":
        return s.queryDataShareByTo(APIstub, args)
    default:
        return shim.Error("Invalid Smart Contract function name.")
    }
}
```

The *queryDataShareByTo()* function shares the patient data with the doctor as per specification received.

6.3 eHealthChain client application

In Hyperledger Fabric, the external world interacts with the fabric network and chaincode using a client application. This interaction is facilitated through Hyperledger SDK using languages Java and Node. Being a permissioned blockchain platform, every participant including a client application must be authorized to interact with the fabric network. A Certificate Authority in the eHealthChain network provides appropriate certificate for a client application to participate.

The client application consists of the logic to interact with the fabric network and the chaincode. The client application interacts with the peer nodes for record approval and with the orderer nodes for block generation respectively. For this purpose, the access point of peers and orderers, as well as the channel name and chaincode name, are to be specified by the client application. Similarly, the client application should supply the correct function name and required arguments while performing query or invoking the chaincode.

The eHealthChain client application is developed on Android platform using Java language. As shown in the Fig. 9, the client application supports various functionality such as registration of doctor and patients, performing OAuth2.0 flow with the health-IoT device backends and showing health record on the mobile device. The client application also allows a patient to authorize

viewing of health records to a doctor based on patient consent.

6.4 eHealthChain Hyperledger Explorer

eHealthChain Explorer is a Web application based on Hyperledger Explorer to view network information (name, status, list of nodes), query blocks, transactions and associated data, chain codes and record families, as well as any other relevant information stored in the ledger. Figure 10 shows the dashboard of eHealthChain Hyperledger Explorer.

7 Conclusion and future work

Due to the proliferation of medical IoT devices in the consumer market, increasing amount of personal health data is being generated. A Personal Health Information Management System (PHIMS) is necessary to allow an individual to gather, store, update, and share personal health data as well as control access to personal health data in a secure and privacy-sensitive manner. Blockchain technology has a potential to help in personalized, authentic, and secure healthcare by merging the entire real-time clinical data of a patient's health and presenting it in an up-to-date secure healthcare setup. However, in order to use blockchain technology for the implementation of PHIMS, additional components are required to collects data from the medical IoT device backend store and transfer it to the blockchain for storage. In this paper, we presented eHealthChain—a
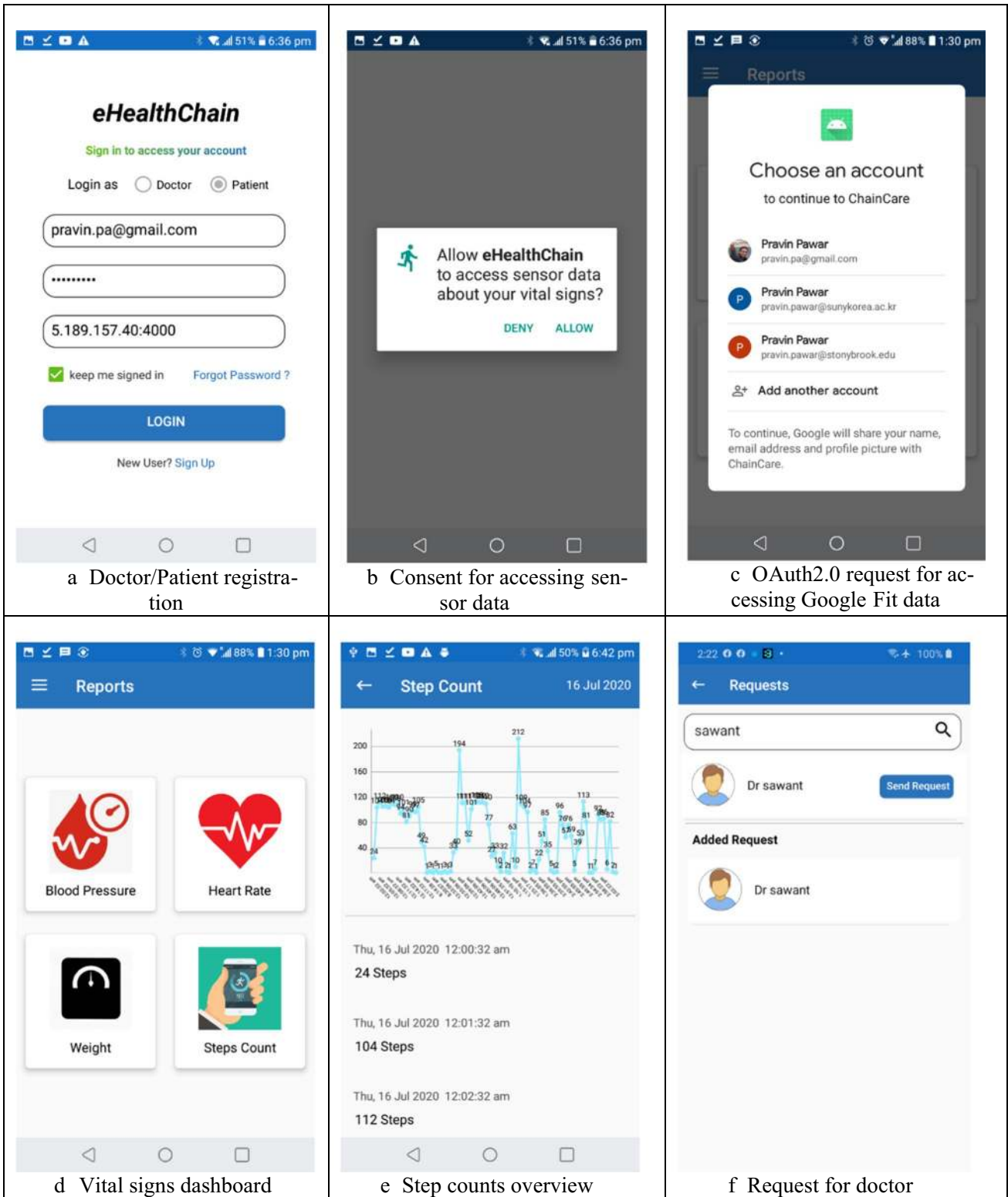
Fig. 9 eHealthChain client application screenshots. **a** Doctor/patient registration. **b** Consent for accessing sensor data. **c** OAuth2.0 request for accessing Google Fit data. **d** Vital signs dashboard. **e** Step counts overview. **f** Request for doctor.
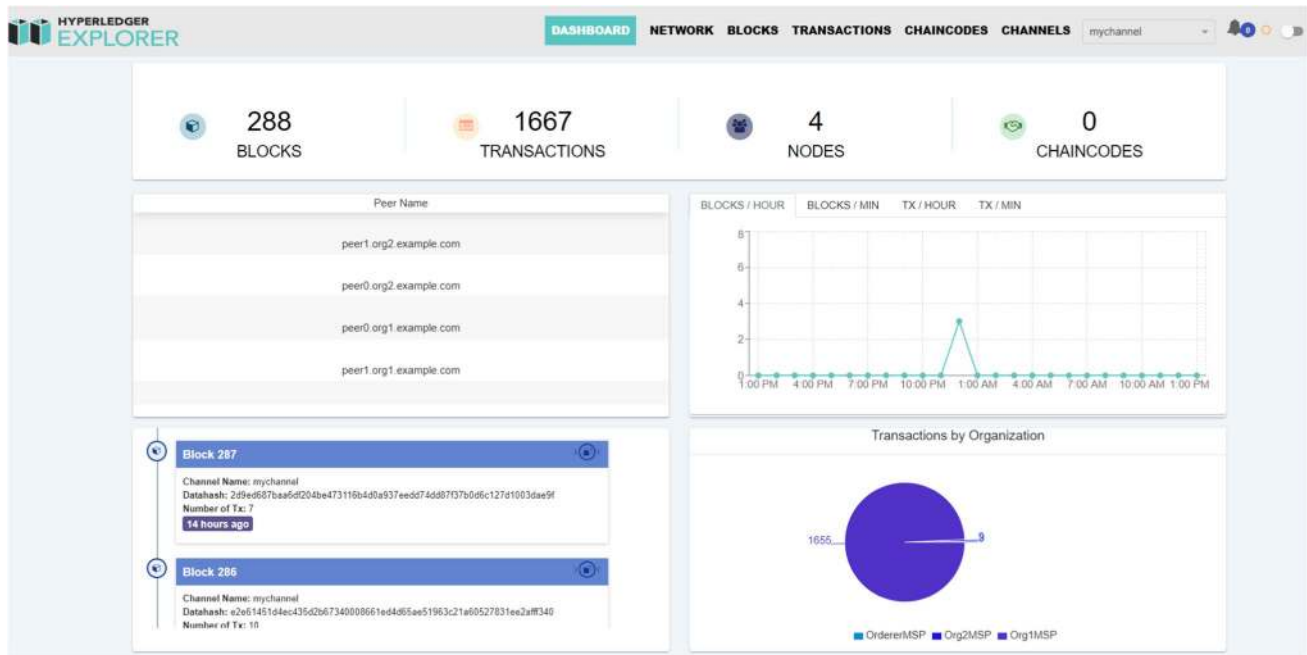
Fig. 10 The dashboard of eHealthChain Hyperledger Explorer

blockchai-based PHIMS, which consists of multiple layers for managing data originating from medical IoT devices and applications. The eHealthChain heavily focuses on an adapter component that collects data from the health device backend and transfers it to the blockchain for storage. The eHealthChain system architecture is extensible to accommodate several medical IoT devices and applications and it is language and platform agnostic. Compared to existing systems such as MedRec which use blockchain for the storage of health data, the health record is provided by doctors, while in the eHealthChain system, health record is provided by an individual whereas individual's health data is obtained using medical IoT devices and applications. We have also presented implementation of the eHealthChain system that uses Hyperledger Fabric as a blockchain platform to store personal health data acquired from devices such as Qardioarm blood pressure monitor, RENPHO digital weighing scale and Google Fit application.

Since data interoperability is one of the major issues in using blockchain technology, our future work is focused on how to extend eHealthChain system with an interoperability layer to allow sharing personal health data with external electronic health record systems. The use of HL7 Fast Health Interoperability Resources (FHIR) standard for sharing health record data will be a valuable addition to the eHealthChain system.

References

1. Teng XF, Zhang YT, Poon CC, Bonato P (2008) Wearable medical systems for p-health. IEEE reviews in Biomedical engineering 1:62–74
2. Pawar P, Jones V, Van Beijnum BJF, Hermens H (2012) A framework for the comparison of mobile patient monitoring systems. Journal of biomedical informatics 45(3):544–556
3. Jovanov E, Talukder BMS, Schwebel DC, Evans WD (2018) Design and feasibility of a safe pill bottle. Applied System Innovation 1(2):13
4. Rogueda P, Grinovero M, Ponti L, Purkins G, Croad O (2019) Telehealth Ready: Performance of the Amiko Respiro Sense connected technology with Merxin DPIs. J Aerosol Med Pulm Drug Delivery 32(2):A26–A26
5. Sargunam B (2019) IoT based mobile medical application for smart insulin regulation, In 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–5, IEEE
6. Civan A, Skeels MM, Stolyar A, Pratt W (2006) Personal health information management: Consumers' perspectives, In AMIA Annual Symposium Proceedings (Vol. 2006, p. 156), American Medical Informatics Association
7. Edemekong P, Annamaraju P, Haydel M (2020) Health insurance portability and accountability act (HIPAA), StatPearls
8. Loayza A (2019) Personal information management systems: a new era for individual privacy?, iapp PrivacyTech
9. Shafagh H et al. (2017) Towards blockchain-based auditable storage and sharing of IoT data, Proceedings of the 2017 on Cloud Computing Security Workshop, ACM
10. Engelhardt MA (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review, 7(10)

11. Martíez I, Escayola J, Martínez-Espronceda M, Munoz P, Trigo JD, Munoz A, García J (2010) Seamless integration of ISO/IEEE11073 personal health devices and ISO/EN13606 electronic health records into an end-to-end interoperable solution. Telemedicine and e-Health 16(10):993–1004

12. Lee BM, Ouyang J (2014) Intelligent healthcare service by using collaborations between IoT personal health devices. International Journal of Bio-Science and Biotechnology 6(1):155–164

13. Rajput DS, Gour R (2016) "An IoT framework for healthcare monitoring systems", . Int J Comput Sci Inf Sec 14(5):451

14. Zgheib R, Conchon E and Bastide R (2017) Engineering IoT healthcare applications: towards a semantic data driven sustainable architecture, In eHealth 360° (pp. 407–418), Springer

15. Gaggioli A et al (2013) A mobile data collection platform for mental health research. Pers Ubiquitous Comput 17(2):241–251

16. Adjerid I, Adler-Milstein J, Angst C (2018) Reducing medicare spending through electronic health information exchange: the role of incentives and exchange maturity. Inf Syst Res 29(2):341–361

17. Jones B, Yuan X, Nuakoh E, Ibrahim K (2014) Survey of open source health information systems. Health Inform 3(1):23–31

18. Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G (2019) Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography 3(1):3

19. Azaria A, Ekblaw A et al. (2016) Medrec: using blockchain for medical data access and permission management, In 2016 2nd International Conference on Open and Big Data (OBD), IEEE, August

20. Wood G (2014) Ethereum: a secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper

21. Al Omar A, Rahman et al. (2017) Medibchain: a blockchain based privacy preserving platform for healthcare data, In International conference on security, privacy and anonymity in computation, communication and storage (pp. 534–543). Springer

22. Ichikawa D, Kashiyama M, Ueno T (2017) Tamper-resistant mobile health using blockchain technology, JMIR mHealth and uHealth, 5(7)

23. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST (2018) FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J 16:267–278

24. Bataineh AS, Mizouni R, Bentahar J, El Barachi M (2019) Toward monetizing personal data: a two-sided market analysis, Future Generation Computer Systems

25. Norta, D. Hawthorne and S. L. Engel (2018) A privacy-protecting data-exchange wallet with ownership- and monetization capabilities. 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, 1–8, doi: https://doi.org/10.1109/IJCNN.2018.8489551.

26. Parra-Arnau J (2017) Pay-per-tracking: a collaborative masking model for web browsing. Information Sciences 385:96–124

27. Javaid A, Zahid M, Ali I, Khan R, Noshad Z, Javaid N (2019) Reputation system for IoT data monetization using blockchain, in Advances on Broad-Band Wireless Computing, Communication and Applications (Lecture Notes in Networks and Systems), Cham, Switzerland: Springer, pp. 173–184

28. Suliman A, Husain Z, Abououf M, Alblooshi M, Salah K (2018) Monetization of IoT data using smart contracts. IET Networks 8, pp. 32–37

29. Singh M (2020) Blockchain Technology for Data Management in Industry 4.0. In: Rosa Righi R., Alberti A., Singh M. (eds) Blockchain Technology for Industry 4.0. Blockchain Technologies. Springer, Singapore. https://doi.org/10.1007/978-981-15-1137-0_3

30. Kundu A, Ayachitula A, Sistla N (2020) Similarities and learnings from ancient literature on blockchain consensus and integrity. arXiv preprint arXiv:2006.04487

31. Hyperledger (2020) Hyperledger Fabric release-2.0 Documentation. Available online at https://hyperledger-fabric.readthedocs.io/en/release-2.0/blockchain.html.

32. Greenspan G (2015) Multichain private blockchain-white paper. Last accessed: 12 Jul 2020. Available online: http://www.multichain.com/download/MultiChain-White-Paper.pdf.

33. Hyperledger Composer Tutorials, "Developer tutorial for creating a Hyperledger Composer solution", last accessed in January 2021. Available online: https://hyperledger.github.io/composer/v0.19/tutorials/developer-tutorial.html.

34. Mukherjee P, Singh D (2020). The Opportunities of Blockchain in Health 4.0. In R. Rosa Righi, A. Alberti, & M. Singh (Eds.), Blockchain Technology for Industry 4.0 (pp. 149–164). Springer, Singapore. doi:https://doi.org/10.1007/978-981-15-1137-0_8

35. Singh D, Rajput N (Eds.). (2020). Blockchain Technology for Smart Cities. Springer Singapore. v, 180. doi: https://doi.org/10.1007/978-981-15-2205-5.

36. Pawar P, Park CK, Hwang I, Singh M (2021) Architecture of an IoT and blockchain based medication adherence management system. In: Singh M., Kang DK., Lee JH., Tiwary U.S., Singh D., Chung WY. (eds) Intelligent Human Computer Interaction. IHCI 2020. Lecture Notes in Computer Science, vol 12616. Springer, Cham. https://doi.org/10.1007/978-3-030-68452-5_22