Hitching Medical IoT Devices to Blockchain for Personal Health Information Management

Pravin Pawar, Thierry Oscar Edoh, Madhusudan Singh, and Neeraj Parolia

Abstract Ubiquitous availability of Internet connectivity IoT enabled medical devices and advances in electronic health records have given rise to massive amounts of personal health data. However, being sensitive in nature, there are stringent legal requirements related to the sharing and processing of personal health data. There is a growing trend of using Personal Information Management System (PIMS) to gather, store, manage, and provide secure and privacy-aware access to personal data. Recently, blockchain technology has emerged as a lucrative option for personal health information management. In this chapter, we propose a layered architecture for a blockchain-based PIMS for managing data originating from medical IoT devices. The proposed architecture has four layers as follows: (1) A blockchain layer that provides functionality to implement and host blockchain database; (2) An IoT device layer that consists of electronic data devices such as health watch, weighing scale, and blood pressure measurement sensors; (3) An application layer that collects data from the health devices and displays consolidated data view to the user; and (4) An adapter layer that has a responsibility of interfacing an application layer with the blockchain layer. The proposed architecture is extensible to accommodate additional electronic devices and services and it is also language and platform agnostic. We are currently building a Proof of Concept (PoC) prototype for validating proposed architecture using Hyperledger Fabric platform.

P. Pawar
Department of Computer Science, State University of New York, Incheon, South Korea
email: pravin.pawar@sunykorea.ac.kr

T. O. Edoh
Chair for Applied Software Engineering, Technical University of Munich, Munich, Germany
email: oscar.edoh@gmail.com

M. Singh (✉)
Department of Technology Studies, Endicott College of International Studies, Daejon, Republic of Korea
email: msingh@endicott.ac.kr

N. Parolia
Department of Business Analytics and Technology Management, Towson University, Baltimore, MD, USA
email: nparolia@towson.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

S.-W. Lee et al. (eds.), Blockchain Technology for IoT Applications, Blockchain Technologies, https://doi.org/10.1007/978-981-33-4122-7_10
Keywords Blockchain technology · Hyperledger fabric · Personal information management systems · IoT integration · Adapter design pattern

1 Introduction

As opposed to the traditional hospital-centric model, there is an emerging trend of providing personalized, individual-centric services to the general population. The p-Health paradigm which stands for pervasive and personalized healthcare 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 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.

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 and 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 [6]. This applies to all forms of PHI, including paper, oral, and electronic, etc. Since health data originates from multiple devices provided by multiple manufacturers and follows different formats, it is also heterogeneous.

These considerations have led to the rise of Personal Information Management System (PIMS). PIMS also known as personal data spaces or personal data store has recently emerged out of the necessity to gather, store, manage, and provide secure and privacy-aware access to personal data [6]. In addition to managing personal data, PIMS facilitates compliance with users’ rights to access their individual data as well as also let people allow, deny, or withdraw consent to third parties for access to their personal data, thus facilitating compliance with existing privacy laws [7]. The healthcare industry will benefit immensely from the adoption of PIMS because of the vast amounts of personal and sensitive data they collect [7].
Blockchain technology has 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 [8]. These features make it a lucrative option for personal health information management. In a blockchain, each subsequent block contains a link to the previous one and a signed and validated block contains authorized transactions. Blockchains connect stakeholders directly without requirements for third-party brokers, they are cost-effective and distributed ledgers providing increased accessibility to information [9]. Compared to existing solutions, Blockchain technology provides the ability to make changes safely and transparently from an unlimited number of sources that can be geographically distributed. Moreover, use of blockchain technology ensures that the system is decentralized, each participant has a latest data version as ensured by consensus algorithms, and there is confidence in the validity of each transaction [9].

Figure 1 shows an extended scenario of using blockchain technology for PIMS where multiple health information record systems such as mobile health care, environmental records, medical insurance information, family health record, medicine record, public health, 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.

However, in order to use blockchain technology for the management of medical IoT data, additional components are required for two purposes: firstly, for sending data originating from IoT devices to the blockchain for storage; and secondly, for retrieving data from the blockchain for an individual use. Presently, most of the connected personal health devices come up with their own mobile app which connects...
to the device, obtains data, and stores device data in the backend store. A component that works as an adapter is required which will collect data from device backend store and transfer it to the blockchain for storage. Adapter component is also required to retrieve data from blockchain and send it to the application which provides user-friendly view of stored data. In this chapter, we propose a layered architecture for a blockchain-based personal information management system for managing data originating from medical IoT devices. The proposed architecture focuses on an adapter layer that works as an interface between personal connected devices and blockchain.

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 PIMS for a blockchain-based personal health information management system. Section 4 elaborates architecture of the proposed blockchain-based PIMS and discusses its features. Section 5 discusses current progress in the development of Hyperledger fabric-based implementation of the proposed approach. Section 6 concludes the paper and provides directions for the future work.

## 2 Related Work

A number of approaches have been proposed for managing data originating from personal health devices. Martíez et al. [10] 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. [11] propose an intelligent service model for healthcare on top of data measurement and storage functionality provided by IoT health devices. In order to obtain data from personal health devices, an application-level collaboration protocol is proposed in [11] which receives bio-signals information from the IoT enabled devices. Rajput et al. [12] 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. [13] present a new IoT architecture for healthcare applications with a focus on the principles of weak coupling and of semantic data exchange. The software architecture proposed in [13] is based on a message-oriented middleware driven by semantic Ontology We Language (OWL) messages and has been implemented using a case study of bedsore detection.

An introduction to blockchain technology in the healthcare sector is provided by Engelhardt [9]. Accordingly, blockchain technology is best suited for the storage and sharing of health information because of the following reasons:

1. Healthcare sector is composed of multiple stakeholders (such as patients, doctors, caregivers, and pharmacists).
2. More trust is required between stakeholders than that currently exists.
3. Trust or efficiency increases in the absence of any intermediary.
4. Reliable tracking of health bio-signals is required.
5. For further analysis, bio-signals data need to be reliable over time.
MedRec is one of the first blockchain-based platforms for managing health data proposed by Azaria et al. [14]. MedRec is a decentralized electronic record management system that provides patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Since it is based on blockchain technology, MedRec manages authentication, confidentiality, accountability, and data sharing—crucial considerations when handling sensitive information. MedRec is prototyped on top of Ethereum blockchain [15]. In MedRec system, the health record data is provided by doctors. MediBchain proposed by Al Omar et al. [16] is another patient-centric healthcare data management system that uses blockchain as storage to attain privacy. MediBChain uses cryptographic functions to protect patient’s data and guarantee pseudonymity. In [16], 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. [17]. They developed an 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 comparison to the related work reported in Sect. 2, the novel aspect of our work is that we propose using blockchain technology to create a PIMS that will obtain and store individual’s health data from multiple medical IoT devices available to the consumers where an individual is the provider of data and make this information available to the patient and clinicians in a secure and privacy-sensitive manner.

3 Considerations and Requirements for a Blockchain-Based Personal Health Information Management System

Popular wearable consumer product companies such as Apple, Google can be expected to provide PIMS features in their existing or new mobile apps and integrate blockchain technology. Also, specialized medical device manufacturers such as Omron would be interested in building blockchain-based PIMS applications for data collection. 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 in patient-centered health care delivery models. As the amount of data increases in the PIMS, 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 blockchain provider, PIMS developer, insurance, and public/private health care providers.

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

4 Architecture of a Blockchain-Based Personal Health Information Management System

In the area of software architecture, adapter design pattern is commonly used to allow two subsystems to interact with each other. The use of adapter pattern allows reusability of existing functionality. In the proposed architecture, an adapter component is required which will collect data from device backend store and transfer it to the blockchain for storage. The proposed architecture of PIMS 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 bitcoin blockchain, any entity is able to join and participate as well as view the ledger, blocks and transaction data inside the blocks. Clearly, a public blockchain platform is not suitable for PIMS, as the privacy of health data transactions cannot be guaranteed. 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 [18, 19].

Private blockchains are more suitable for the implementation of PIMS as they allow only authorized entities to join the blockchain network. The frameworks such as Ethereum, HydraChain, and Hyperledger Fabric facilitate developing blockchain applications [20]. Ethereum is one of the popular public blockchain platforms with support for smart contracts allowing applications to run exactly as programmed. HydraChain extends the Ethereum platform by supporting creation of permission blockchain.

Hyperledger Fabric, Multichain [21] are examples of private blockchain platforms. Hyperledger Fabric is a permissioned blockchain framework implementation by The Linux Foundation. The smart contracts in Hyperledger Fabric [20] are called “chaincode” and they comprise the application logic of the system. The external applications can blockchain smart contracts using REST APIs which are exposed by the Hyperledger Fabric and Ethereum platforms.

4.2 Device Layer

The device layer consists of medical IoT devices such as health watch, activity trackers, weighing scale, smart pill bottle, and other sensors. 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 corresponding mobile app. Handheld mobiles also function as health data devices provided that corresponding applications are installed.

### 4.3 Application Layer

The entities at the application layer consist 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 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 also 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 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 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.
4.5 Access of Blockchain-Enabled Personal Health Information Management System (PHIMS)

Patient personal health information can be uploaded by the patient and only authenticated hospital authorities on blockchain-enabled PHIMS. As we can see in Fig. 3, a patient is in charge of updating personal health information and is able to access the information using direct authorization. Patient has an authority to verify other stakeholders such as clinician/nurse/caregiver who has access to patient’s data and vice versa. Since the personal health information management system is based on blockchain technology, it’s data can be accessed using a mutual verification.

5 Hyperledger Fabric Based Architecture of a BlockChain-Based Personal Health Information Management System

In this section, we introduce some key concepts of Hyperledger Fabric followed by a step-by-step approach to create a blockchain for managing personal health data obtained from medical IoT sensors.

Fig. 3 Access to blockchain-enabled PHIMS
5.1 Key Concepts of Hyperledger Fabric

In a blockchain network, a distributed ledger maintains a record of all transactions that are executed in the network. 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. Consensus refers to the process of approving and synchronizing ledger transactions across the network. In the traditional system, the members of a business network transact with each other while maintaining separate records of their transactions. In comparison, in a blockchain network, every participant has own copy of the ledger which is replicated with other participants.

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. The members of Hyperledger Fabric network use a trusted Membership Service Provider for enrolling in the network [22]. 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 transaction 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 transactions are used to modify assets. A Hyperledger Network uses a channel over which the business network participants communicate for ensuring privacy. Hyperledger Fabric allows network participants to choose a consensus mechanism such as Crash Fault-Tolerant (CFT) or Byzantine Fault-Tolerant (BFT) ordering. Figure 4 shows the features of Hyperledger Fabric for supporting management of personal health data.

5.2 Employing Hyperledger Fabric Channel for Sharing Personal Health Data

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 transactions. A channel is defined by members (organizations), anchor peers per member, the shared ledger, chaincode application(s), and the ordering service node(s). Each transaction 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 a Membership Services Provider (MSP), which authenticates each peer to its channel peers and services [22].

For managing patient’s personal health data, there will be multiple members in the business network:
Fig. 4 Features supporting management of personal health data in Hyperledger fabric

1. A blockchain-based PIMS platform that obtains and stores user’s health data;
2. A mobile app that enables a user to obtain data from device backend using OAuth and send this data to PIMS platform for storage; and
3. Other members such as doctors and caregivers who are interested in obtaining user’s health data.

The moment any user registers as a PIMS platform member by using mobile application, it would automatically get connected to Channel 1 which in turn will connect to peer Node of the PIMS Platform. Then PIMS platform’s Certificate Authority would issue the Hyperledger blockchain account by issuing a X.509 certificate to the user by using Membership Service Provider. The X.509 certificate will then get stored in user’s mobile’s application space. The certificate would later be used to sign the transactions or all transaction proposals, when user tries to write or log or update his health record.

Channel 1 is owned and controlled by the PIMS platform as the network initiator. In the case of users or patients, the mobile application would directly get connected to Channel 1 which is created and controlled by an EHR-platform in a blockchain
network. When a user provides consent to doctors/caregivers for accessing the health record, Channel 1 would connect all the members—including users and doctors/caregivers.

All members connected to this channel will share the ledger controlled and governed by the smart contracts deployed to share health records. Here, all the three members PIMS Platform, user, and doctor/caregiver will have shared ledger between them connected through Channel 1.

5.3 Approach for Creating a Personal Health Data Blockchain Using Hyperledger

In the following, we illustrate a systematic approach to create a personal health data blockchain using Hyperledger Composer that builds application on top of Hyperledger Fabric [23]:

- **Step 1**: Define a business network that consists of assets, participants, transactions, access control rules and optionally events and queries [15]. Asset is an important entity whose data is stored in the fabric using a key-value pair, hence all health measurement data are assets. In order to prevent data format issues, we propose using XML or JSON format for storing the data into the blockchain so that authorized participants can retrieve it and convert into their own format. Participants such as patients are members of a business network who own assets and submit transactions which change the state of assets. Queries are used to extract data from the blockchain network. Access control rules allow fine-grained control over what participants have access to what assets and under what conditions.

- **Step 2**: Generate a deployable business network archive from the business network definition created in Step 1.

- **Step 3**: Deploy a business network to the instance of Hyperledger Fabric, start the network, and create a network admin identity that consists of a digital certificate and private key to administer the business network after deployment.

- **Step 4**: Generate a REST server that provides language-agnostic API to develop a web application. The generated API is connected to the deployed blockchain and business network. Given appropriate credentials, REST API can be used for sending data transactions to and receiving data from the deployed backend.

Figure 5 shows an application use-case of employing Hyperledger Fabric for the personal health information management. We are working on the development of end-to-end prototype for hitching medical IoT devices to Hyperledger Fabric blockchain. In this use case, the components of the device layer are medical IoT devices, which are available for purchase in the market. The application layer corresponds to mobile applications and backend cloud store provided by these device manufacturers. The adapter layer consists of programmed components to perform OAuth 2.0-based
Fig. 5 Application use-case of employing Hyperledger fabric for health information management authentication with the device cloud store 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 a mobile app, which provides consolidated view of health data as per patient consent.

6 Conclusion and Future Work

A personal information management system allows an individual to gather, store, update, and share personal data as well as control access to personal data in a secure and privacy-sensitive manner. Recently, blockchain technology is being considered as a lucrative option for personal information management due to its compelling features such as fault tolerant and distributed ledger, irreversible, auditable, time-stamped and cryptographically sealed information blocks and near-real-time information updates. In this chapter, we elicited high-level requirements for a blockchain-based personal health information management system and proposed a layered architecture for managing data originating from personal health devices. The proposed architecture heavily focuses on an adapter component that collects data from the health device backend and transfers it to the blockchain for storage. The proposed architecture is extensible to accommodate additional electronic devices, and it is also language and platform agnostic. In the existing systems such as MedRec which use blockchain for the storage of health data, the health record is provided by doctors, while in the proposed system health record is provided by an individual whereas individual’s health data is obtained using medical IoT devices available in the market. We
have also reported the architecture, design of a proof of concept prototype that uses Hyperledger Fabric blockchain to store personal health data acquired from devices such as Fitbit health watch, QardioCore ECG EKG monitor, and QardioArm blood pressure monitor.

References

1. Teng XF, Zhang YT, Poon CC, Bonato P (2008) Wearable medical systems for p-health. IEEE Rev Biomed Eng 1:62–74
2. Pawar P, Jones V, Van Beijnum BJF, Hermens H (2012) A framework for the comparison of mobile patient monitoring systems. J Biomed Inform 45(3):544–556
3. Jovanov E, Talukder BMS, Schwebel DC, Evans WD (2018) Design and feasibility of a safe pill bottle. Appl Syst Innov 1(2):13
4. Rogueda P, Grinovero M, Ponti L, Purkins G, Croad O (2019) Telehealth ready: performance of the Amiko Respido sense connected technology with Merxin DPIs. J Aerosol Med Pulm Drug Deliv 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). IEEE, pp 1–5
6. Edemekong P, Annamaraju P, Haydel M (2020) Health insurance portability and accountability act (HIPAA). StatPears
7. Loayza A (2019) Personal information management systems: a new era for individual privacy?iapp PrivacyTech
8. Shafaghi H et al (2017) Towards blockchain-based auditable storage and sharing of IoT data. In: Proceedings of the 2017 on cloud computing security workshop. ACM
9. Engelhardt MA (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innov Manage Rev 7(10)
10. 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
11. Lee BM, Ouyang J (2014) Intelligent healthcare service by using collaborations between IoT personal health devices. Int J Bio-Sci Bio-Technol 6(1):155–164
12. Rajput DS, Gour R (2016) An IoT framework for healthcare monitoring systems. Int J Comput Sci Inf Secur 14(5):451
13. Zgheib R, Conchon E, Bastide R (2017) Engineering IoT healthcare applications: towards a semantic data driven sustainable architecture. In: eHealth 360°. Springer, pp 407–418
14. 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
15. Wood G (2014) Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper
16. Al Omar A, Rahman MS 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. Springer, pp 534–543
17. Ichikawa D, Kashiyama M, Ueno T (2017) Tamper-resistant mobile health using blockchain technology. JMIR mHealth and uHealth 5(7)
18. Jayachandran P (2017) The difference between public and private blockchain. IBM Blockchain Blog, Blockchain Pulse
19. Whitaker MD, Pawar P (2020) Commodity ecology: from smart cities to smart regions via a
blockchain-based virtual community platform for ecological design in choosing all materials
and wastes. In: Blockchain Technology for Smart Cities. Springer, pp 77–97
20. Nagpal R (2017) 17 blockchain platforms — a brief introduction. Medium Blockchain blog
21. Greenspan G (2015) Multichain private blockchain-white paper. https://www.multichain.com/
download/MultiChain-White-Paper.pdf
22. Hyperledger (2020) Hyperledger fabric release-2.0 Documentation. https://hyperledger-fabric.
readthedocs.io/en/release-2.0/blockchain.html
23. Hyperledger Composer Tutorials (2020) Developer tutorial for creating a Hyperledger
composer solution. https://hyperledger.github.io/composer/v0.19/tutorials/developer-tutorial.
html