Sharing Wearable Health Data Using User-Defined Blockchain Policies

Alan Colman[1(✉)], Mohammad Jabed Morshed Chowdhury[2], and Mohan Baruwal Chhetri[1,3]

[1] Swinburne University of Technology, Melbourne, Australia
acolman@swin.edu.au
[2] Latrobe University, Melbourne, Australia
m.chowdhury@latrobe.edu.au
[3] CSIRO Data61, Melbourne, Australia
mohan.baruwalchhetri@data61.csiro.au

Abstract. With recent advances in wearable technology and the rapid adoption of wearable devices, there are increased opportunities for setting up innovative data markets through which large amounts of user-generated physiological data can be made available to health researchers at relatively low costs. However, given the sensitive nature of such data, a major challenge associated with realizing a trusted wearable data marketplace is ensuring fine-grained access control and assuring conformance to it. In this paper, we propose a policy-based approach for facilitating the secure exchange of data between a wearable owner and a health researcher. User-defined data-sharing policies are translated into executable smart contracts that provide deterministic and transparent execution of transactions as per the terms and conditions of the data sharing agreement. To illustrate feasibility of the approach, we present a proof-of-concept implementation of the proposed policy-based access control mechanism using the open source Multichain platform.

Keywords: Wearable data · Blockchain · Data sharing policy

1 Introduction

With recent advances in wearable technology and the rapid adoption of wearable devices [1], we are witnessing a paradigm shift in the way personal physiological data is generated, stored and consumed. There are increased opportunities for setting up innovative markets where user-generated health data can be made available for consumption in real-time or batch mode, and at relatively low costs. However, given the sensitive nature of such data, there are several challenges associated with running wearable data markets while safeguarding the consent, security and privacy of all market participants. In particular, the owners of the wearables, referred to as *data subjects* in our terminology, should have full control over how their wearable data is shared with others, including which parts

P. Perego et al. (Eds.): ICWH 2020, LNICST 376, pp. 54–69, 2021.
https://doi.org/10.1007/978-3-030-76066-3_5

of the data is shared, under what context, and with whom. More importantly, they should have assurances that their data is shared in conformance with their data-sharing policies.

In our previous work [2], we presented an approach for building a consortium-based trusted marketplace for wearable data. In that paper we showed how blockchain technology can fulfil many of the requirements associated with creating trust between remote and unknown parties participating in a transaction. The requirements that we considered in that work include fairness, transparency, privacy, security and auditability. We further presented a high-level conceptual architecture showing how transactions related to the sharing of wearable data could be facilitated by a blockchain-based marketplace in accordance with the terms and conditions stipulated by the wearable user.

In this paper we extend our previous work on a general policy language for data sharing [3] that enables individuals to control access to their shared data based on context, device types and data types. In doing so, we make the following main contributions:

- We analyse various access modes provided by the main wearable device manufacturers that can enable third-party access to wearable data (Sect. 3).
- We show how data sharing policies can be applied to the sharing of wearable health data. User-defined data-sharing policies are translated into executable smart contracts on a blockchain that provide deterministic and transparent execution of transactions based on agreed terms (Sect. 4).
- We describe an architecture and protocols that enable researchers *(data consumers)* to securely access a wearable owner's *(data subject's)* bio-data from cloud storage provider's API *(data custodian)* in conformance with the owner's data sharing policy (Sect. 5.1).
- We present a proof-of-concept of the proposed system using the Multichain platform [4] and discuss the various trade-offs in implementing such systems (Sect. 5.2).

The rest of the paper is organized as follows. Section 2 provides background information on blockchain-based wearable data markets. Section 3 summarises the different access modes to wearable data while Sect. 4 provides an overview of the policy language for user-controlled wearable data sharing. It also provides a description of how the access control mechanisms work. Section 5 briefly describes the system design and implementation. Section 6 concludes the paper.

2 Background and Related Work

2.1 Wearable Devices in Medical Research

The use of wearable devices has proliferated in recent years. These devices include ubiquitous smartphones, smart watches and wrist bands that can monitor personal physiological data. Novel devices such as chest straps, electronic garments, skin patches, smart glasses, even smart jewellery are starting to emerge.

Seneviratne et al. [1] provide a recent survey of such devices. In the clinical medical domain, these devices are used to monitor vital signs such as heart rate, blood pressure, respiratory rate, blood oxygen saturation, and body temperature [5]. Personal monitoring devices are widely used in hospital settings. They are also being increasingly used for monitoring the condition of patients on discharge – in particular patients with chronic conditions such as diabetes and cardiovascular illness. Much work has been done to integrate such wearable Patient Care Devices (PCDs) with hospital information systems and electronic health records, and in developing interoperability standards for such integration [6]. Devices used in such clinical contexts typically tend to be expensive industry grade monitors.

The use of such devices in medical research, however, is a nascent field. These devices not only allow the researchers to collect and gather real-time data coming from individuals who can be profiled, but the fine-grained frequency of the data also makes it possible to reveal insights and correlations that were impossible or difficult to perceive previously. Of course, any inaccuracies in consumer devices used for research would affect the accuracy of the research results. However, given that the accuracy of sensor types can be characterized, it is established practice to model such inaccuracies and adjust for them in the interpretation of results. That being said, recent studies have shown that consumer wearable devices often have an accuracy compatible with clinical-grade devices [7]. As technology develops it can be expected that the accuracy of consumer devices will continue to improve.

However, while the use of wearables in health research studies may not pose any immediate clinical risk to the research subject's health, there are considerable risks to privacy through exposing identifiable personal data. Such devices are not only capable of recording physiological data but also typically record additional information such as the wearer's location. It is therefore paramount that any platform developed to acquire such data ensures that it is kept private by using anonymization [8] or encryption [9].

2.2 Blockchain

A blockchain is an immutable distributed ledger for recording transactions. Its transactions are called immutable because once inserted, they become permanent and cannot be modified retroactively, not even by the authors, without the alteration of all subsequent transactions. Having records added to the blockchain requires a consensus mechanism that ensures the transactions are confirmed as valid. A blockchain is secured by cryptographic techniques and managed by a decentralized community over a peer-to-peer network. These properties have made blockchain technology a suitable platform for enabling trust in transactions between parties who do not necessarily trust each other.

There are, however, many types of blockchain that vary according to the openness of the network, the type of transactions recorded, and the mechanism by which consensus is achieved. Blockchain technology gained prominence through Bitcoin which is an open system that records simple cryptocurrency

transactions between untrusted participants. Participants are pseudo-anonymous in that their identity on the network is a public encryption key rather than a real-world identity. Consensus amongst participants in such open blockchains is reached through incentivized mechanisms such as proof-of-work [10].

Other types of blockchain platforms (e.g. Hyperledger[1]) enable blockchains to be formed by a consortium of participants. These *permissioned* blockchains are more common in facilitating cross-organisational collaboration between participants in an industry (e.g. supply chain tracking). Access to participation in the blockchain is defined by various roles. For example, certain members may be the only ones allowed to participate in consensus making while others may only have rights to participate in transactions. Depending on the level of trust between consortium members, consensus in permissioned blockchains can be typically realised through simpler mechanisms, such as simple majority voting. Depending on the implementation, participants may have pseudo or real-world identities visible to others on the blockchain. In general, if the blockchain is tracking activities in the real-world (rather than just virtual transactions between cryptocurrency accounts stored on the blockchain), real-world identities need to be able to be established for enforcement purposes (if not necessarily publicly visible).

The nature of transactions may also vary between types of blockchain. While crypto-currencies like BitCoin merely track the balances of accounts to establish if a transfer is valid, platforms like Ethereum[2] have generalised the mechanisms for making valid transactions in the form of *smart contracts*. Such contracts are immutable code stored on the blockchain that gets executed by the participants to a transaction. While there are various names for, and approaches to implementing such contracts, in this paper we use the term *smart contract* in the general rather than Ethereum-specific sense. Transactions on a blockchain can also be classified as *on-chain* or *off-chain*. In on-chain transactions, the validity of the transactions is only dependent on the state of the blockchain itself (e.g. does the payer have enough crypto-currency on the blockchain to make a transfer). In off-chain transactions, the blockchain facilitates and tracks the transfer typically through the exchange of encryption keys.

In terms of the above distinctions, the type of blockchain relevant to the data sharing platform we describe in this paper is a permissioned blockchain whose voting members are a consortium of research institutions. The blockchain stores access control agreements between data providers and data consumers as smart contracts. The blockchain is the decision point that controls and tracks data access, as well as facilitating payments from the data consumer to the data subject (wearable owner). While the blockchain creates a channel for the off-chain transfer of the wearable data, this data itself is not stored on the blockchain. It also gives participants in a sharing agreement visibility to the terms of the instance of the smart contract to which they are a party, along with a record of any transactions executed under that contract.

[1] https://www.hyperledger.org/.
[2] https://ethereum.org/.

2.3 Blockchain-Based Health Data Sharing

There has been a lot of work on blockchain based healthcare data sharing as evidenced by the numerous recent literature surveys [11–15]. Researchers have looked at using blockchain for a number of different data sharing scenarios including genomic data sharing [16], medical imaging data sharing [17], electronic medical record (EMR) sharing [18], clinical trial data sharing [19], and wearable data sharing [2].

In [16], the authors have proposed blockchain as the enabling technology for DNA brokerage. EncrypGen[3] is a commercial DNA data marketplace built on top of Multichain that gives individuals control over their personal DNA data and how it is sold to other users, researchers and companies. MedRec [18] is a blockchain based electronic medical record (EMR) management system proposed by researchers from MIT. It allows health care providers to share medical records amongst themselves and with their patients. Health care providers maintain control over the patient data which is stored on their servers, but provide controlled access to the data by entering into patient-provider relationships. The system is built on top of the Ethereum blockchain. [20] is another research proposal that proposes a consortium-led blockchain-based system for the secure sharing of medical big data between hospitals. Researchers from UCLA have proposed a private blockchain-based platform for sharing medical imaging data between data providers, physicians and personal health record vendors [17]. Similarly, Nugent et al. [19] have proposed a framework to improve data transparency in clinical trials using blockchain smart contracts. They have showed that smart contracts can act as trusted administrators, which can improve the transparency of data reporting in clinical trials. In [21], the authors propose a purpose-centric access model leveraging the blockchain to enables patients to own, control and share their healthcare data with untrusted third-parties without violating privacy. They also point out the secure multi-party computing is a promising solution to enable untrusted third-party to conduct computation over patient data without violating privacy. In [22], Benchoufi et al. explore the core functionalities of Blockchain that can be leveraged for conducting reliable clinical trials including patient enrolment, data collection, trial monitoring, data management and data analysis.

Our work differs from the above mentioned approaches in that we focus on continuously generated physiological data captured by data subject owned wearable devices as opposed to EMRs, medical images and one-off measured DNA data. We have previously proposed a blockchain based wearable data marketplace [2] where the main objective is to provide wearable owners complete control over how their physiological data is shared with unknown (and potentially untrusted) parties in an semi-trusted environment. We combine blockchain technology with policy-based management to address some of the issues associated with running a wearable data marketplace including fine-grained access control, privacy-preserving data sharing, confidentiality-preserving data sharing,

[3] https://encrypgen.com/.

auditable data sharing, integrity-preserving data sharing and fair and secure data exchange. The work in [23] is similar to our approach in that it proposes a blockchain based personal health data sharing system. However, the authors do not provide any details on (a) how the data consumers can achieve fine-grained access control over their data, (b) how data consumer requirements are matched with the available health data sets, and (c) how they address the issue of trust between untrusted data consumers and data owners.

3 Accessing Data from Wearable Devices

There are different types of wearable devices, however they largely follow the same steps in terms of flow of data. First, different types of sensors, such as motion, blood pressure, heart-rate continuously generate data. This data is temporarily stored on the wearable then typically transferred to a smart phone (unless of course the sensor is in the smart phone). User applications on these devices allow the owner to monitor the current or historical data.

At this point, approaches of vendors vary in terms of whether or not the data is uploaded to the vendor's cloud. Wearable device vendors usually provide SDKs to enable the development of apps for wearables to directly collect and send data. In the case of smartphones, tablets and PCs, SDKs are available to develop apps that collect data directly from wearable devices. Using these SDKs, third-parties can develop specific applications to collect data on wearables and send it to other applications. Cloud services usually provide REST APIs. These REST APIs allow third-parties to gain access to users' data stored in the cloud. Using these two options, it is possible to gain access to wearable data. Individuals can also delegate access to this data via these APIs. However, some of the wearable vendors provide both SDK and REST API and some only provide one option.

Below is the list of main wearable platforms and their data access methods:

- **Apple Health.** Apple Health is made up of both local storage and cloud services, an app, and a SDK (Health Kit). The Apple Health local storage and cloud services maintain all the data collected from users and provide some analytic services. Nevertheless, Apple Health does not provide any REST API for third-party systems.
- **Google Fit.** It provides both SDK and API to provide access to the stored data in the google cloud. It provides a SDK for app developers, a SDK to gain access to Google Fit local storage (device storage) and REST APIs for third-party systems. The Android app is needed to transfer the data from the wearable to the smartphone and then to the cloud servers.
- **S-Health.** Like Google fit, a mobile app is required to synchronize the data with the Samsung server. It also provides a SDK to support the development of apps by third-party developers, gaining access to collected data in the proprietary local storage (SDK-Warehouse). Nevertheless, this SDK does not enable the access to wearable data sensors directly. The S-Health platform does not include any REST API.

- **Fitbit.** It only provides REST API for third-party systems. This platform synchronizes data from Fitbit quantification bands and enables third-party developers to get such data through the REST API. Fitbit also provides SDK to allow the application developers to facilitate access to the fitbit cloud.
- **Microsoft Health.** It provides a SDK for app developers and a REST API for third-party systems. Using these two facilities it is possible to gain access to data available in the Microsoft cloud that has been collected from Microsoft Band devices.

In summary, there are two ways in which the data generated by the wearable devices can be accessed. Option 1 is to access the data via APIs and option 2 is to directly access the data from the devices via mobile apps.

3.1 Access to Wearable Data by Third Parties

In this paper we assume data from the wearable device has been uploaded to the vendor's or other cloud either automatically or via mobile app. We call the provider of this cloud the *data custodian*. To directly share access to their data with a third party the wearable owner (*data subject*) needs to provide credentials (e.g. access keys) to access that data. However, the data subject does not want to provide the data consumer access to *all* their wearable data on an ongoing basis. OAuth [24] is the de-facto access control mechanism for the REST APIs based data sharing. OAuth enables users to grant access to their data and process to third parties without disclosing the user's authentication data. Generally, OAuth provides to clients (used by data consumer) a "secure delegated access" to server resources (usually cloud service) on behalf of the individuals. Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. There are usually different types of APIs published by the vendors to share different types of data. OAuth token generated for any particular API works for that particular API only. For example, heart rate API by fitbit (https://api.fitbit.com/1/user/5Buser-id5D/activities/heart/date/5Bdate5D/5Bperiod5D.json) allows wearable owners to share their heart rate data and the OAuth token for this API can only be used to retrieve heart-rate data.

One of the major limitations of access delegation via mechanisms such as OAuth is that it is binary decision based access. That means either individuals have to give access to the resource or deny access. They do not have any fine-grained control over access. For instance, they cannot control access based on the context (e.g., time, location). In the next section we describe a policy schema that enables a data subject to define rules for fine-grained access to their data, and show how this schema can be incorporated into smart contracts that govern the sharing/sale of that data. We have described how the OAuth protocol can be combined with the user-defined data sharing policy to provide more fine grained control to the individuals over their data sharing in Sect. 5.1.

4 Data Sharing Policy Schema

We have proposed a general data sharing policy schema in our previous work in [3]. We have also defined the main roles involved in the trading of wearable data including the *Data Subject* who the data refers to, the *Data Consumer* who wants access to that data, and *Data Custodian* who holds the data on the Data Subject's behalf [2]. Below, we describe how the general data sharing policy schema can be applied to wearable data sharing.

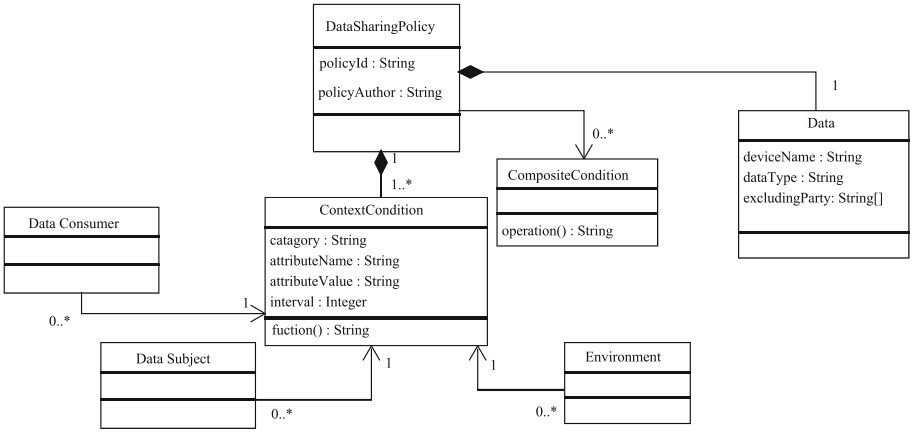

Fig. 1. Meta-model of data sharing policy.

The context and identity of the data consumer is captured by the attributes. For instance, location based access control is expressed as the location of either data subject or data consumer (e.g., dataSubject.location). Data is expressed using three attributes, namely deviceType, dataType and accessPoint. *deviceType* allows to define the types of device – in the case of wearables devices such as Apple Watch, Fitbit etc. *dataType* defines the types of data – in the case of wearable data parameters such as heart-rate, blood-pressure, sleeping pattern etc. *accessPoint* is the web address (e.g., URI) of the data access point often is the API end points. *excludingParty* defines if there is any party with whom the data subject does not want to share the data, such as military. Figure 1 shows the meta model of the data sharing schema, which consists of two elements, namely, context condition and data. *Context condition* allows the data subject to define different types of contextual requirements such as time context (e.g., 9 am to 5 pm). The *Data* element allows to define device types, data types, and excluding party (e.g., military). Listing 1.1 show the an example data-sharing policy.

4.1 Encoding Policy for Smart Contract Services on Blockchain

Blockchain ensures the immutability of the code or data. That means nobody can edit or delete any information from the blockchain network. In addition to that it

ensures that what is written in the blockchain is always enforced in transactions on the blockchain. The way blockchain ensures that is typically through a *smart contract*. Depending upon the blockchain platform used, it can also be referred to as chain-code and smart filter. A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.

In our mechanism, the user-defined policies giving consent to data access are a key part of the smart contract stored on the blockchain that ensures the consent defined by the data subject is always checked and enforced. The policy itself is encoded and stored in the blockchain as JSON format [25]. The following is a sample policy stored in the blockchain.

Policy: *Share my blood-pressure data from fitbit from 10th of February to 15th of February excluding military purpose.* Listing 1.1 represents the JSON encoding of the above policy.

Listing 1.1. Policy Definition of Scenario Using Concrete Syntax

```
"dataSharingPolicy" : {
    "policyId" : "222",
    "author" : "Tanya",
        "ContextCondition" : {
         "function" : "greater-than-or-equal"
                "category" :  "environment"
                "attributeName" : "date"
                "attributeValue": "10-02-2020"  },{
                "function" : "less-than-or-equal"  {
                "category" :  "environment",
                "attributeName" : "date"},{
                "attributeValue": "15-02-2020"
        },
        "Data" : {
            "deviceName" : "fitbit",
            "dataType" : "blood-pressure",
            "excluding" : "military",
            }}
```

4.2 Data Sharing Contracts

A policy defines *what* wearable data the data subject is prepared to share and any context constraints they want imposed on that sharing – for example, *when* they are prepared to share and with what type of consumer. When the data subject makes an offer to sell their data, they also specify a price. When this offer is accepted by a data consumer it constitutes a contract of sale. The contract contains the agreement between the data subject and the data consumer and includes the asking price and the data sharing policy.

After a contract is created, it is linked with the data subject, broker and data consumer via their wallet id (which is the public key address in the blockchain).

Listing 1.2 shows the JSON encoding of a smart contract corresponding to the example data policy presented in Listing 1.1. The wallet id (public key) of the data subject is used to transfer payment from the data consumer to the data subject. Finally, the blockchain module namely, "*fetcher*" retrieves the individual's wearable data from the data custodian based on this contract. This contract is implemented as a *"smart contract"* or as we say a *"smart filter"* in terms of Multichain platform. As this is implemented as smart contract, blockchain always ensures that this contract is always enforced.

Listing 1.2. Template for Contract (Smart Contract)

```
"Contract" : {
    "subject-wallet-id" : "MIGfMA0GCSqGSIb3DQEBAQBgQCqGKuk",
    "broker-wallet-id" : "NMMafsdfhkhsdfSI4GNAkKBgQCqGKuk",
    "consumer-wallet-id" : "Ikdfsakfhsadkjfhshhjfhsdkjdfd",
    "price" : "5",
    "policy" : {
          "function" : "greater-than-or-equal"
                "category" :  "environment"
                "attributeName" : "date"
                "attributeValue": "10-02-2020"  },{
                "function" : "less-than-or-equal"
                "category" :  "environment",
                "attributeName" : "date"},{
                "attributeValue": "15-02-2020"
                "deviceName" : "fitbit",
                "dataType" : "blood-pressure",
                "excluding" : "military"
              }}}
```

5 System Design and Implementation

A prototype of the system has been implemented using microservices and the MultiChain blockchain platform. In this section we will briefly describe the high level architecture of the system, and then discuss how this was implemented as a proof-of-concept prototype.

5.1 Architectural Design

Figure 2 shows a high-level view of the system run by a Consortium of research institutions, and how this system interacts with the wearable's owner, the APIs of the custodian (wearable manufacturer) who holds the data, and the health researcher who wants access to the data.

From Fig. 2, it can be seen there are two main data flows. The sequence of flow is indicated by the numbers in circles. The first data flow is that of the bio

data itself as indicated by large brown arrows. Bio data is sent from the wearable device to the Data Custodian's cloud storage ① where such APIs are provided (as with FitBit and Google Fit), or third party storage that acquires the custom data through an app with appropriate SDKs (e.g. Apple Health) as discussed in Sect. 3. The Research Consortium's Fetcher service then securely accesses a user's data via an API provided by the Data Custodian ⑦. As we will discuss below, access to this data is controlled by a smart contract based on the Broker-mediated business agreement reached between the wearable Owner/user and the Health Researcher. The bio data is then anonymised and filtered if necessary ⑧ before being passed on to the Health Researchers ⑨.

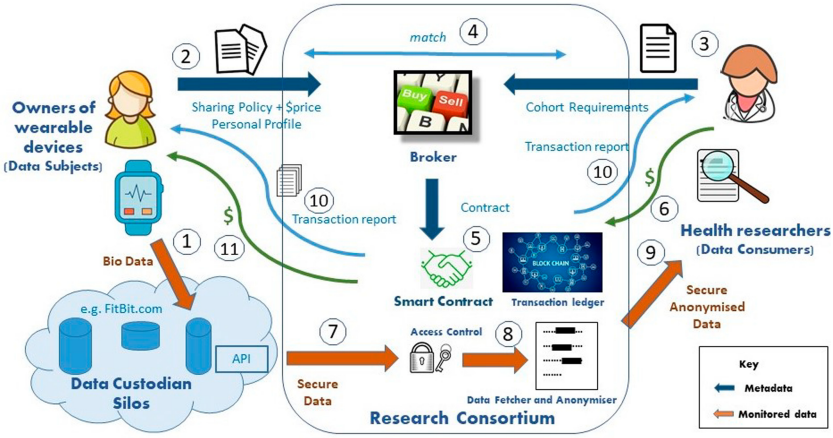

Fig. 2. A high level system architecture

The other main data flow represents the transactions that enable secure exchange of data according the smart contract agreement. This data flow is indicated by the large blue arrows in Fig. 2. Both the Owner and the Health Researcher interact with the system through client web apps. The Owner makes an offer to provide (or sell) their data using the provided web app ②. The Owner uses the form on the web app to specify an access consent policy that details what data they wish to sell, including the source, parameters (such as heart rate, BP, activity) and time window. To illustrate a screen shot from the prototype Owner Web App is shown in Fig. 3.

The user also provides a personal profile (age, sex, etc.), and nominates the price (if any) they want for their data. The Health Researcher uses a separate web app to specify the type of wearable data that they are interested in, the cohort from which they want this data, and the price if any they are prepared to pay ③. The Health Researcher can also specify the frequency with which they want the data from the Data Custodian. For much research, retrieving the data in large batch would be appropriate as the researcher is interested in

historical data. However if the system is to be adapted to a clinical setting, then the data consumer could set the frequency of polling to a very short interval to achieve near real-time updates.

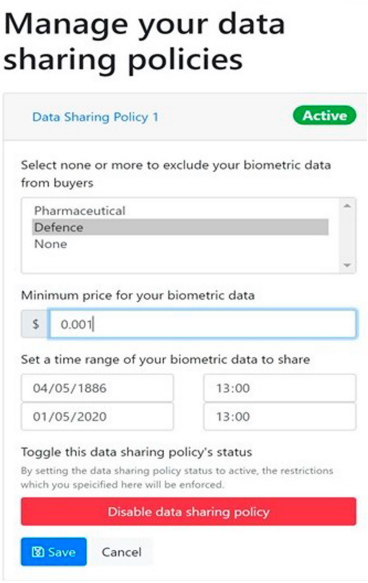

Fig. 3. Wearable owner web app: user-defined sharing policy and offer

The role of the Broker within the research consortium is to match buy offers from researchers with (multiple) sell offers for wearable health data ④. As well as matching data parameters the broker is, if required, matching the cohort requirements of the researcher with the personal profiles provided by the data subjects. This profile and cohort information is for matching purposes only and stays confidentially with the broker. The real identities of the participants also remain confidential to the broker with only the pseudo-identities (wallet ids) being exposed. When matches are found, the broker writes the policy, the wallet ids and the agreed price into a contract (as discussed in Sect. 4) onto the Consortium's blockchain ⑤ where they are visible to the parties to that contract for auditing.

These contracts are the control points that govern access to that data from the custodian's API. Once a contract is in place, a data channel is created by the Consortium's Fetcher service. This channel runs from the custodian's API, through the intermediate steps of anonymisation and filtering, to an end-point provided to the data consumer. The data consumer does not get direct access to the API. The data can then either be pulled by a consumer request, or pushed to the consumer.

While the Broker is assumed to be a trusted part of the Consortium in the above schema, in the more detailed design described below we have implemented the Broker as a separate service. This would enable the possibility of creating a marketplace with several competing for-profit brokers vying to match wearable data providers and consumers (although this then may create trust issue between the Consortium and the brokers).

The ancillary data flows in light arrows in Fig. 2 are directly handled by the Consortium's blockchain. They involve (micro)payments from the Health Researcher to the Consortium ⑥ and from the Consortium to the Owner (11), and reporting of transactions to the parties to the contract ⑩. The payment flow is optional. For example, if the health researcher works for a university that is a Consortium member, the consortium may not charge for that data. Similarly, a device owner may be happy to provide their data for gratis if they see it being used for the public good.

5.2 Implementation

A proof of concept prototype has been implemented using MultiChain [4], an open source blockchain platform suitable for deploying private (permissioned) blockchains across organisations. As a permissioned blockchain, MultiChain gives fine-grained access-control to users with various levels of authority within the blockchain using a very extensive permission system[4]. This fine-grain user-access control was a primary reason for choosing MultiChain over other permissioned blockchains such as the Ethereum-based Quorum[5]. In our case, owners, researchers and consortium members all have different level of access. Owners and researchers can only see contracts and transactions to which they are party. This allows parties to audit their own transactions without being able to breach the privacy of other participants. Being a permissioned system, consensus for confirming transactions does not need to rely on expensive mechanisms like proof-of-work. Rather, custom mechanisms for reaching consensus (e.g. simple majority) can be implemented amongst nodes with sufficient privileges, in this case the consortium institution members. Each member institution of the research consortium needs to configure a MultiChain node. In the prototype we have simulated these nodes running of separate VMs in a private cloud.

MultiChain uses 'smart filters' similar to the 'smart contracts' in Ethereum or 'chain code' as with HyperLedger. While the implementation of these contracts/filters varies depending on the platform, they all immutably define the transaction rules of a chain—in our case encoding the agreed policy contract. In this paper we have used the term 'smart contract' in a generic sense rather than referring to specific Ethereum concept. The Fetcher component of the Consortium system then uses this contract to securely retrieve the specified data. These transactions are recorded on the chain.

[4] https://www.multichain.com/developers/permissions-management/.
[5] https://www.goquorum.com/.

One limitation of blockchains is their limited ability to store large amounts of data. However, in our case this does not present a problem as the bio data and user profile data does not actually pass through the blockchain. Rather, the blockchain is controlling the access mechanism for that data. MultiChain also supports the transfer of assets enabling value exchange if that is required by the system. However, enabling crypto-currency transactions via the blockchain would require parties to have appropriate crypto-coin wallets. This may prove an impediment to the widespread adoption of the system. The alternative which we implemented in the prototype was to have the blockchain track a nominal asset value that maps to a fiat currency and externalise the payment mechanism.

As each custodian of wearable data is likely to have their own API for authenticate access and data retrieval, adaptors need to be added to mediate the interactions. In the prototype implementation we created adaptors for FitBit and Google Fit to successfully retrieve data as specified in policy contracts.

6 Conclusion

In this paper, we presented a policy-based approach for the secure, transparent and privacy-preserving exchange of wearable data between wearable device owners and health researchers. The data subjects can specify fine-grained access control over how their data is shared including which parts of the data is shared, under what context and with whom. When these policies are matched with the requirements specified by the data consumers, the resulting agreements get translated into executable smart contracts on the blockchain that ensure that consent as defined by the data subject is always checked and enforced thus facilitating data exchange between parties who are remote and potentially unknown to each other. We have implemented a proof-of-concept prototype of a wearable data marketplace using the open source Multichain platform in which smart filters are used to enforce data exchange in conformance with the data-sharing policies specified by the wearable owners.

As future work, we would like to explore some of the key challenges associated with realising wearable data marketplaces including ensuring the integrity and confidentiality of the wearable data. For example, how can data consumers be assured that the data they purchase is coming from *bona fide* wearables worn by subjects whose profile matches the cohort requirements. Similarly, how can data subjects be assured that the data consumer will not share their data with others without their explicit consent.

Acknowledgement. We acknowledge the contributions of our students, Paul Sarda and Andrew Davis from Swinburne University of Technology.

References

1. Seneviratne, S., et al.: A survey of wearable devices and challenges. IEEE Commun. Surv. Tutor. **19**(4), 2573–2620 (2017)

2. Colman, A., Chowdhury, M.J.M., Chhetri, M.B.: Towards a trusted marketplace for wearable data. In: 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), pp. 314–321. IEEE (2019)
3. Chowdhury, M.J.M., Colman, A., Han, J., Kabir, M.A.: A policy framework for subject-driven data sharing. In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018)
4. MultiChain: MultiChain—Open source blockchain platform (2019). https://www.multichain.com/
5. Dias, D., Cunha, J.P.S.: Wearable health devices–vital sign monitoring, systems and technologies. Sensors **18**(8), 2414 (2018)
6. Rhoads, J.G., Cooper, T., Fuchs, K., Schluter, P., Zambuto, R.P.: Medical device interoperability and the integrating the healthcare enterprise (IHE) initiative. Biomed. Instrum. Technol. (Suppl), 21–27 (2010)
7. El-Amrawy, F., Nounou, M.I.: Are currently available wearable devices for activity tracking and heart rate monitoring accurate, precise, and medically beneficial? Healthc. Inform. Res. **21**(4), 315–320 (2015)
8. Bayardo, R.J., Agrawal, R.: Data privacy through optimal k-anonymization. In: 21st International Conference on Data Engineering (ICDE 2005), pp. 217–228. IEEE (2005)
9. Chowdhury, M.J.M., Pal, T.: A new symmetric key encryption algorithm based on 2-d geometry. In: 2009 International Conference on Electronic Computer Technology, pp. 541–544. IEEE (2009)
10. Lo, S.K., et al.: Analysis of blockchain solutions for IoT: a systematic literature review. IEEE Access **7**, 58822–58835 (2019)
11. Cyran, M.A.: Blockchain as a foundation for sharing healthcare data. Blockchain in Healthcare Today (2018)
12. Hathaliya, J.J., Tanwar, S.: An exhaustive survey on security and privacy issues in healthcare 4.0. Comput. Commun. **153**, 311–335 (2020)
13. Khezr, S., Moniruzzaman, Md, Yassine, A.: Blockchain technology in healthcare: a comprehensive review and directions for future research. Appl. Sci. **9**(9), 1736 (2019)
14. Mackey, T.K., et al.: 'Fit-for-purpose?'-challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med. **17**(1) (2019). Article number: 68
15. McGhin, T., Choo, K.-K.R., Liu, C.Z., He, D.: Blockchain in healthcare applications: research challenges and opportunities. J. Netw. Comput. Appl. **135**, 62–75 (2019)
16. DeFrancesco, L., Klevecz, A.: Your DNA broker. Nat. Biotechnol. **37**(8), 842 (2019)
17. Patel, V.: Secure and decentralized sharing of medical imaging data via blockchain consensus. Technical report, Department of Radiological Sciences, University of California, Los Angeles (2016)
18. Azaria, A., Ekblaw, A., Vieira, T., Lippmanm, A.: MedRec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30. IEEE (2016)
19. Nugent, T., Upton, D., Cimpoesu, M.: Improving data transparency in clinical trials using blockchain smart contracts. F1000Research **5** (2016)
20. Cheng, X., Chen, F., Xie, D., Sun, H., Huang, C.: Design of a secure medical data sharing scheme based on blockchain. J. Med. Syst. **44**(2) (2020). Article number: 52. https://doi.org/10.1007/s10916-019-1468-1

21. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**(10) (2016). Article number: 218. https://doi.org/10.1007/s10916-016-0574-6
22. Angeletti, F., Chatzigiannakis, I., Vitaletti, A.: The role of blockchain and iot in recruiting participants for digital clinical trials. In: 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–5. IEEE (2017)
23. Zheng, X., Mukkamala, R.R., Vatrapu, R., Ordieres-Mere, J.: Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1–6. IEEE (2018)
24. Hardt, D., et al.: The OAuth 2.0 authorization framework. Technical report, RFC 6749, October 2012
25. Shin, S.: Introduction to JSON (JavaScript object notation). Presentation (2010). www.javapassion.com