Phonendo: A Platform for publishing wearable data on DLT

Francisco Moya[0000−0002−1282−9268], Luis Martínez[0000−0003−4245−8813], and Fco Javier Estrella[0000−0002−3170−5543]

Universidad de Jaén, Spain {fpmoya,martin,estrella}@ujaen.es

Abstract. Modern intelligent health-based software nowadays is based on data-driven systems that collect data streams from wearable devices that perform continuous remote monitoring of patient parameters. The importance of such wearable devices and data streams is key because of their low cost, but also because they facilitate the building of a large number of solutions to multiple health-based problems. Despite of the easy manipulation of both, devices and their data streams; the necessary processes from collecting data to final analyses passing by data transformation and variable creation present an important flaw such as, it is the security of such data in applications that is mandatory. Distributed Ledger Technologies (DLT) enable systems to be endowed with characteristics such as resistance to information manipulation or resilience to the appearance of single points of failure. DLT have the potential to build wearable-based solutions offering characteristics that would allow building a wider range of possible solutions. This contribution introduces Phonendo, a platform for collecting data streams from wearable devices and publishing them on a DLT Infrastructure (DLTI). Phonendo is under development and here we focus on the presentation and justification of its interface layers, i.e., data collection and publication on a DLTI.

Keywords: IoT · Wearable · Telemedicine · DLT.

1 Introduction

Wearables and **I**nternet **o**f **T**hings (**IoT**) devices are main elements for designing novel intelligent computing services that can successfully address various health and well-being issues [5, 14]. Nowadays there exist a wide heterogeneity of available devices and sensors, as well as computer based solutions categorised as IoT. However, a precise deficion of IoT is not simple and different definitions for IoT have been provided in the specialised literature [2, 18, 20] that tried to delimit the IoT either from the characteristics of its constituent elements [20], the typology of communication that characterises it [18], its enabling aspects for the creation of certain types of applications [4] or even from a temporal perspective in which the ratio of objects connected to the internet versus people is considered [11]. For our contribution, we focus on the use of wearable devices, understood as a subset of IoT devices, according to [20].

Wearable devices allow obtain and process individual health parameters such as heart rate, body temperature, cardiovascular pressure, glucose levels and so forth; that makes such devices particularly useful for developing solutions in the field of health [14] because the values collected for previous parameters can be used in raw or processed, for the detection of complex activities such as physical exercise, sleep cycles, anxiety episodes, cardiac crises or loss of consciousness [8].

In spite of the good features and advantages provided by wearable devices for health based solutions, it must be pointed out that IoT devices in general and wearable devices in particular suffer from security problems [25], that hinder the development of all promising health services based on wearable devices.

Consequently, in order to avoid such security problems has recently emerged a trend that explores the use of **D**istributed **L**edger **T**echnology (**DLT**) [12, 24] and its promise of resistance to information tampering and resilience to single points of failure, seeking to alleviate some of the existing security problems.

Consequently, this contribution aims at studying the applicability of DLTs to a real-world wearable scenario, mainly focus on securing the collecting, storing and publishing of health wearable based data. Hence, we propose a platform so-called **Phonendo** that allows to pair wearable devices, collect their data streams and publish them on a DLT infrastructure, commonly referred as **DLT I**nfrastructure (**DLTI**) [1].

The Phonendo platform goes beyond this contribution due to its complex architecture to achieve the objective of developing and deploying new products meeting the requirements of health based services. Therefore, in this contribution we just focus on its interface layers, which deal with collecting data and publishing them on the most appropriate DLTI.

The remaining of the contribution is structured as follows. Section 2 reviews the main concepts used for the discussion of the proposal. Section 3 refers to the potential benefits and limitations of using DLTs in this scenario and introduces some possible applications. Section 4 presents the Phonendo architecture, reviewing each service in detail and makes a justification of its design decisions. Finally, Section 5 presents conclusions and future work.

2 Background

This section briefly revise some necessary concepts about IoT and DLT to understand our proposal and some related works about the use of DLT to solve any of the problems regarding IoT environments are provided.

2.1 IoT

IoT is a pervasive technology, although it presents many security issues [25] that make it difficult to use in real-world environments. Its solutions have the ability

[1] Note that the acronym DLT refers to a technology while the acronym DLTI refers to the deployment of an infrastructure using this technology.

to affect various aspects of human life, that can be mainly categorised into four domains [6]: i) Transport and logistics. ii) Smart environments. iii) Social and personal applications. iv) Healthcare.

IoT solutions are affected and sometimes limited by different facts:

- **Huge amount of data and/or nodes**. The number of IoT devices is huge and constantly increasing. In turn, each device generates a large amount of data during its lifetime.
- **Decentralisation**. Due to the large number of nodes that can coexist in an IoT network and their communication [23].
- **Unstable and unpredictable connections**. It is common in IoT solutions because of the quantity and heterogeneity of devices.

The features of IoT based solutions and their devices may lead to the emergence of several technological weaknesses and hence to potential attacks on such applications [25], such as attacks on (i) end devices, (ii) communication channels, (iii) network protocols, (iv) sensors, (v) denial of service or (vi) software. In this context, multiple authors are analysing DLTs to deal with them [17, 21].

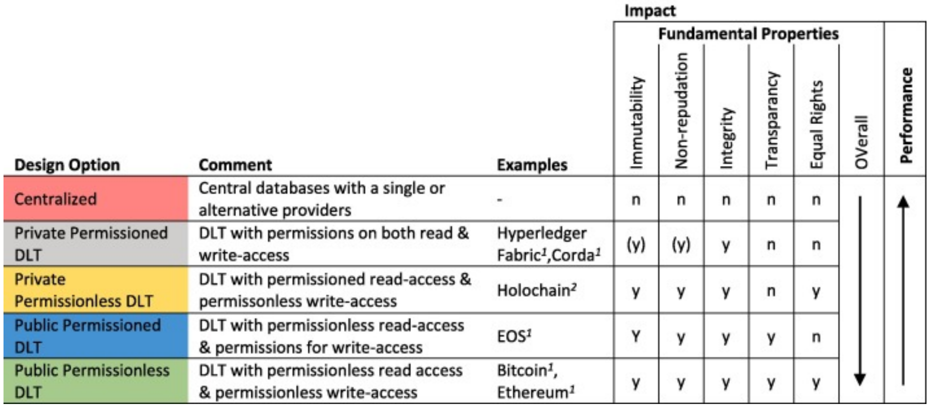
2.2 DLT

Briefly, DLT can be defined as a technology that uses transactional databases that exist across multiple locations or between multiple participants and that may or may not use a central authority to process, validate or authenticate information transactions. Some authors describe its main characteristics [19]:

- **Shared copy**. The entities maintain a shared set of records called **ledger**.
- **Consensus**. The entities agree on the update of the ledger.
- **Network participation design**.
  - **Permissioned**. Participation requires prior authorisation.
  - **Permissionless**. Participation does not require prior authorisation.
- **Independent validation**. Each entity can verify the integrity of the ledger.
- **Tamper detection attribution**. Each entity can detect non-consensual changes.
- **Inmutability**. An entity cannot alter past records.

Consensus is one of the more challenging points in a distributed system. It consists in achieving an agreement among a number of nodes and achieving fault-tolerant systems. The result of the decision reach is considered final and cannot be reversed. Over the years, different consensus algorithms for DLT have been published in the literature, nowadays we can find different taxonomies depending on the characteristics of the algorithm [15], but most of them require proof to validate the authenticity.

Another key point is the DLT design, there are different alternatives depending on the nature of the ledger (public / private) and the network participation design (permissioned / permissionless). Xu et al. in [27] analysed different combinations and, from that analysis, they got as result in the table in Figure 1, comparing all alternatives with a central database approach.



			Impact						
			Fundamental Properties						
Design Option	Comment	Examples	Immutability	Non-repudation	Integrity	Transparancy	Equal Rights	OVerall	Performance
🟥 Centralized	Central databases with a single or alternative providers	-	n	n	n	n	n	↓	↑
Private Permissioned DLT	DLT with permissions on both read & write-access	Hyperledger Fabric[1],Corda[1]	(y)	(y)	y	n	n		
Private Permissionless DLT	DLT with permissioned read-access & permissonless write-access	Holochain[2]	y	y	y	n	y		
🟦 Public Permissioned DLT	DLT with permissionless read-access & permissions for write-access	EOS[1]	Y	y	y	y	n		
🟩 Public Permissionless DLT	DLT with permissionless read access & permissionless write-access	Bitcoin[1], Ethereum[1]	y	y	y	y	y		

Fig. 1. DLT design alternatives vs central database approach. 1. Examples by Ballandies et al. [7]: Ethereum, EOS, Hyperledger Fabric, and Corda. 2. Example by Daniels [10]: Holochain.

2.3 Related Works

Different proposals about DLTI and DLT solutions for securing IoT scenarios are briefly revised below.

Infrastructure
It can be generally considered that a DLTI adapted to an IoT scenario will also be adapted to a wearable scenario, and the specific needs of wearable devices can be solved with second layer solutions.

Sengupta J. et al. in [21] provided a comprehensive review in which, main issues of an IoT scenario and recent theoretical proposal were analysed. However, at present, most of the DLTIs reviewed have only been theorised and cannot yet be used to develop solutions based on them.

Among the available DLTIs that claim to deliver value in an IoT scenario, two approaches prevail: (i) those that incorporate specific characteristics for the IoT, such as VeChain or WaltonChain [21], and (ii) those that, due to their greater scalability or capacity to manage large volumes of small data, are more adapted to the type of information existing in an IoT scenario, such as IOTA [17], IOST or Streamr [21].

Solutions
In [13] was addressed the use of DLT to improve the security and data analysis from wearable devices in healthcare by proposing a DLT framework adapted to the computational capabilities of the devices.

Meanwhile, in [22] was addressed similar issues to the studied in [13] and also explores how to adapt DLT to the low performance of wearable devices, using a **P**roof **o**f **W**ork (**PoW**) protocol based on **D**irected **A**cyclic **G**raphs (**DAG**).

Also with a focus on health, in [16] was proposed the use of DLT to create a framework for health records using data obtained from wearable devices.

In [9] was proposed an architecture based on a trust model that seeks to increase the privacy of users who provide information from wearable devices.

Finally, in [26], the use of DLT in conjunction with **A**rtificial **I**ntelligence (**AI**) to deal with chronic diseases in a wearable environment is proposed, with DLT serving as a reliable means to ensure user privacy and facilitate information sharing and AI as an engine for analysing data and making suggestions for action.

3 Scenario Applicability Study

Before introducing Phonendo, this section provides an analysis of the impact of publishing information on a DLTI as well as the adaptation of a DLTI to a wearable scenario. Finally, some potential applications and their limitations will be studied.

3.1 Impact of a DLTI on Data Storing

Storing data on a DLTI enables the development of solutions that will have characteristics such as (i) resistance to alteration and/or deletion of data, (ii) resistance to alteration of write time stamps, (iii) resistance to provider identity spoofing o (iv) resilience to single points of failure.

Characteristics (i) and (ii) are acquired through the use of a distributed ledger that is modified under a decentralised consensus process, (iii) through the use of asymmetric cryptographic mechanisms such as digital signatures and (iv) by using distributed systems.

It should be noted that the use of a **D**istributed **F**ile **S**ystem (**DFS**) such as **IPFS**[2] could be a valid alternative to the use of a DLTI if the data is only collected due to its subsequent evidential value. However, it should be considered that a DFS would either (i) lose some of the characteristics offered by a DLTI or (ii) require additional actions to achieve equivalent characteristics:

1. Using a DFS will simplify conceal information.
2. Using a DFS will simplify the generation of multiple values for a single read in order to subsequently selectively disclose a particular value.
3. Solutions such as IPFS do not guarantee the availability of a specific value, being necessary that there are availabe nodes with copies of this value. To prevent data loss, own nodes or dedicated services must be used.

Additionally, certain DLTIs allow the use of **S**mart **C**ontracts (**SC**), a kind of computer programs with the terms of the agreements between different entities that are self-executed when specific conditions are met. Support for SC enables the development of decentralised applications that, to highlight some of the possibilities they offer, would make it possible to (i) implement crypto-economic

[2] https://ipfs.io/

models to incentive the provision of information, (ii) allocate non-fungible tokens to prove participation in the system, (iii) develop marketplaces to monetise individualized or aggregated data, or (iv) define decentralised autonomous organisations.

3.2 Adapting to a Wearable Scenario

Adapting Architecture to Wearable Devices
Wearable devices are characterised according to [6] by (i) low computational resources, (ii) small data payloads, (iii) recurrent data capture, (iv) sensitive data, (v) different hardware specifications, (vi) different communication protocols, (vii) use in scenarios where multiple devices are used at the same time, and (viii) easy attackability.

Thus, a platform that exposes an architecture adapted to these devices must take into consideration their characteristics and be adapted to them.

Selection of the Most Appropriate DLTI
The analysis of the most suitable DLTI for the platform we wanted to propose was not been focused on the limitations of DLTIs but on the features of our proposal that we want to strengthen and the possible solutions that could be built using it.

Maybe, the crucial point in this selection is the use of a permissioned DLTI versus a permissionless one [27]. Generally, a permissioned DLTI, in which the ledger is modified by a limited set of authorized participants who reach consensus in a non-competitive manner makes it possible to reduce operational costs, optimize the ledger's performance, minimize the nodes' computational resources and increase control over access to information. On the other hand, a permissionless DLTI facilitates the verification of information for all types of entities and enables third party users to build their own applications using this information.

This contribution seeks to make the framework useful in scenarios where transparency, energy efficiency, and performance are key factors. Regarding privacy, a permissionless DLTI fits better with our proposal for transparency. Regarding energy efficiency and performance, the Phonendo platform employs IOTA [17], which has very high energy efficiency [3] and performance/scalability due to its nature. IOTA is a DAG-based DLTI that offers a set of features unusual among permissionless DLTIs:

- **No commission costs on writing**. Users are not required to have any tokens to publish.
- **Reduced latency to add information**. In IOTA there are no blocks which gives the infrastructure great write throughput.
- **Libraries**. The IOTA ecosystem offers several libraries of special relevance for the development of our platform, specifically **Identity** [1], a framework for the **S**elf-**S**overeign **I**dentity (**SSI**), and **Streams** [1], a framework for the creation of communication channels that may or may not be encrypted.

[3] https://blog.iota.org/energy-consumption-of-iota-2-0

- **Support for SC.** Recent versions of IOTA introduce support for SC through the **I**OTA **S**mart **C**ontract **P**rotocol (**ISCP** [1]).

These features make IOTA unique in terms of efficiency and performance and therefore a highly suitable DLTI for our platform. Nevertheless, its use raises two significant issues:

1. Due to its feeless nature, its ledger increases in size quickly. To address this, a process of balance snapshot and instantiation of a new ledger is performed periodically. To retrieve historical information a **Permanode** [1] is required.
2. As a SPAM prevention mechanism, IOTA requires PoW per transaction. If the publishing device has limited computational resources, it should delegate the PoW to a third party.

Remark both problems lie in the use of IOTA's public network and not in the use of its technology. Thus, it would be possible to deploy a hypothetical DLTI using its technology and limit itself to storing only data relevant to the domain in which we will deploy the solution and, at the same time, decrease or suppress the PoW per transaction. However, it is easy to reason that (i) in case of not limiting access, this hypothetical DLTI could be easily attacked and that (ii) in case of limiting access, there would be no difference with respect to a permissioned DLTI.

3.3 Potential Applications and Limitations of Solutions

Our hypothesis is that having a platform with the characteristics mentioned in Section 3.1, that is, resistance to alteration and/or deletion of data, resistance to alteration of write time stamps, resistance to provider identity spoofing and resilience to single points of failure, makes it possible to conceptualise applications that can benefit from the value added by this platform, especially in healthcare:

1. **Validation of medical studies**. It would be possible to guarantee that the data have not been manipulated and are true reflection of the study carried out.
2. **Clear up responsibilities**. It would be possible to determine the start time of an episode requiring health-care action, who is involved on it and to provide more transparency. From this information it would be possible to measure important aspects such as the reaction time of the health services or to clear up responsibilities if something goes wrong facing an emergency situation.
3. **Health research**. It would be possible to offer quality information for studies, understanding quality in this context as the veracity of the data information available.
4. **Certification of medical conditions**. It would be possible to perform activities such as stress tests on elite athletes in controlled environments and proof them to a third party.

5. **Incentivise the performance of healthy activities**. It would be possible to establish gamified systems that incentives the performance of activities.
6. **Information sharing between different entities**. It would be possible for a user to give access to his/her historical records to different entities in a secure mode.

However, we must be aware that although solutions such as the above could be easily conceived, it is important to consider that the fact that a solution is technically feasible does not imply that is useful in the real world.

First of all, it is possible to demonstrate that any of the characteristics listed at the beginning of Section 3.2 can be defeated by employing different attacks[4]. Therefore, a data-driven solution should not be built if the cost of attacking it is lower than the potential benefit of doing so.

In addition, any solution focused on collecting data should be reconsidered if, for it to work properly, it is necessary for participants to provide the data whether it benefits or harms them, especially if the data can be manipulated prior to publication.

Finally, and taking into consideration the type of data collected by wearable devices, solutions should be avoided if the information may pose a risk to user's privacy even if the information can be encrypted before being stored.

Note that these limitations are not specific to the proposed platform, but general to any platform with similar characteristics. The ideal scenarios for the implementation of solutions will be those that combine one or more of the following characteristics:

- Individuals have not direct control over the readings of the wearable devices they use and the wearable devices are provided to them ready to use.
- The devices are used under the monitoring of an impartial supervisor.
- The data collected do not generate a detriment to the individual using the devices and there are no desirable or undesirable values for them.
- The correct use of the devices is beneficial to the wearer.

4 Phonendo Platform

Phonendo is a platform made up of services for collecting data from wearable devices and publishing it on IOTA. This contribution just focuses on its interface layers of data collection and publication, although it should be noted that there are still open lines of work focused on the use of SSI and homomorphic computing in order to secure the solutions and facilitate the analysis of the captured data. Because the development is not completely finished, we cannot provide empirical support with results data from an applicable use case to this contribution.

Phonendo platform is being actively developed and it is hosted and accesible via Github [3]. It is composed of several repositories, one repository for each service. In 4.1 platform and each service architecture will be described in detail.

[4] 51% attacks on certain DLTs for (i) and (ii), social engineering attacks for (iii), or denial of service attacks for (iv).

4.1 Architecture

In order to maximise the flexibility of the platform to adapt to the environments in which it is deployed, as well as to adapt to the characteristics of wearables, among which low computational capacity and criticality of information prevail, the functionality is divided into five services, whose interconnections and main functionalities are illustrated in Figure 2.

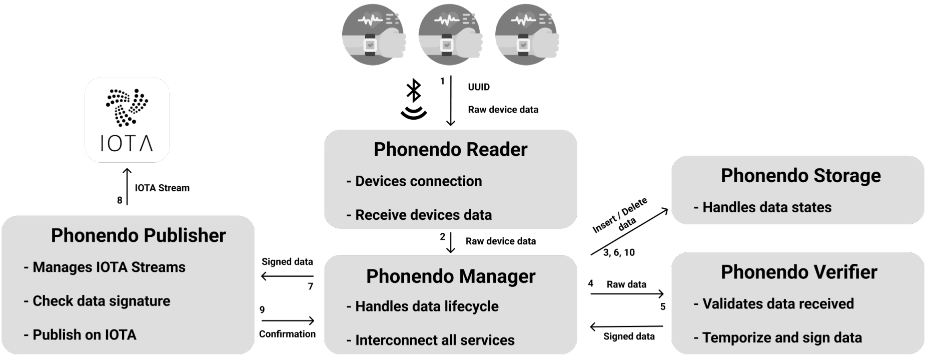


Fig. 2. Phonendo Architecture

In addition, a number of technical decisions have been taken:

- Each service has been developed using the programming language most appropriate for the functionality to be provided.
- **LibP2P**[5] is used for communication between the services.
- The current development focuses on the integration of smartwatches. These (i) provide access to values such as heart rate or sleep cycles and (ii) typically use Bluetooth as the communication protocol, which is widely spread. Given the restrictions introduced by several manufacturers in these devices, **Pine Time**[6] is used as a reference device for development.

4.2 Services

We will now describe the services of the architecture shown in Figure 2 and the state of development of the architecture.

Phonendo Reader

It is the gateway to the system and is responsible for managing the connection with the senders and receiving their data. The platform allows multiple instances of it to exist in order to adapt to the needs of the solutions to be deployed. In

[5] https://libp2p.io/

[6] https://www.pine64.org/pinetime/

order to minimise its computational needs and allow it to run on IoT gateways deployed on low-cost single-board computers, it has been developed using Rust. Development in progress.

Phonendo Manager
This service manages the life cycle of the data, from its capture to its publication, initiating its operations when a Reader instance notifies it of a new piece of data. For simplicity of development, the programming language used was Node.js. Development completed.

Phonendo Storage
This service allows (i) modelling information and (ii) controlling the state of a data in the operational flow. To maximise flexibility in handling different data typologies as well as a potential replacement of the underlying database engine, the service has been developed using Node.js. In its current implementation, the database engine used is LevelJS[7]. Development completed.

Phonendo Verifier
This service implements heuristics to validate the integrity of the data, generating as a result of its execution a signed message that time-stamps the capture of the information. To facilitate the development of new heuristics in the future, it has been developed using Node.js. Development completed.

Phonendo Publisher
This service manages the publication on the IOTA [1] streams where the messages generated by Phonendo Verifier are published. Since this service will have to deal with the PoW required by IOTA for transactions, it has been developed using Rust in order to optimise its computational efficiency. Development in progress.

4.3 Data Flow

Once the previous services have been briefly reviewed, the ideal data flow in the platform is illustrated. Note that the steps are outlined in Figure 2 and such steps as private key creation and management are omitted for sake of clarity.

1. **Matching**. The wearable devices are registered in Reader. Once they are valid senders they will start sending data.
2. **Data reception**. Reader notifies Manager when data is received.
3. **Data processing**. Manager requests Storage to model the data, obtaining as a result a JSON document. Internally, Storage stores this information and sets its status to 'Captured'.
4. **Verification**. Manager requests Verifier to verify and sign this document, resulting in a signed JSON document.

[7] https://leveljs.org/

5. **Status Update: Verified**. Manager notifies Storage of the data verification, and Storage updates the status.
6. **Data publication**. Manager requests the publication to Publisher, obtaining as a result the confirmation of the publication in IOTA.
7. **Status Update: Published**. Manager notifies Storage of the publication, which performs the removal from the database.

5 Conclusions and Future Work

In this contribution, the Phonendo platform has been presented and its information capture and publication interface layers have been described. In order to adapt its architecture to its use with wearable devices, an analysis of this scenario has been carried out.

Phonendo is a platform under development and at present, aspects such as information encryption, access regulation, query resolution or the possibility of generating analytical information from the available information have only been covered briefly, and a further detailed analysis of each of these aspects will be necessary in future research.

References

1. The complete reference for iota, https://wiki.iota.org/. Last accessed 31 July 2022
2. Correcting the iot history, http://www.chetansharma.com/correcting-the-iot-history/. Last accessed 31 July 2022
3. Phonendo source code, https://github.com/orgs/dltcafe/teams/phonendo/repositories. Last accessed 31 July 2022
4. That internet of things thing, https://www.rfidjournal.com/that-internet-of-things-thing. Last accessed 31 July 2022
5. Abboushi, B., Safranek, S., Rodriguez-Feo Bermudez, E., Pratoomratana, S., Chen, Y., Poplawski, M., Davis, R.: A review of the use of wearables in indoor environmental quality studies and an evaluation of data accessibility from a wearable device. Frontiers in Built Environment **8** (2022). https://doi.org/10.3389/fbuil.2022.787289
6. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks **54**(15), 2787–2805 (2010). https://doi.org/10.1016/j.comnet.2010.05.010
7. Ballandies, M.C., Dapp, M.M., Pournaras, E.: Decrypting distributed ledger design—taxonomy, classification and blockchain community evaluation. Cluster computing **25**(3), 1817–1838 (2022)
8. Chen, L., Hoey, J., Nugent, C.D., Cook, D.J., Yu, Z.: Sensor-based activity recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) **42**(6), 790–808 (2012). https://doi.org/10.1109/TSMCC.2012.2198883
9. Chowdhury, M.J.M., Ferdous, M.S., Biswas, K., Chowdhury, N., Kayes, A., Watters, P., Ng, A.: Trust modeling for blockchain-based wearable data market. In: 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). pp. 411–417 (2019). https://doi.org/10.1109/CloudCom.2019.00070
10. Daniels, A.: The rise of private permissionless blockchains—part 1 (2018)

11. Dave, E., et al.: How the next evolution of the internet is changing everything. The Internet of Things (2011)
12. Du, Y., Wang, Z., Leung, V.C.M.: Blockchain-enabled edge intelligence for iot: Background, emerging trends and open issues. Future Internet **13**(2) (2021). https://doi.org/10.3390/fi13020048
13. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for iot. Sensors **19**(2) (2019). https://doi.org/10.3390/s19020326
14. Huhn, S., Axt, M., Gunga, H.C., Maggioni, M.A., Munga, S., Obor, D., Sié, A., Boudo, V., Bunker, A., Sauerborn, R., Bärnighausen, T., Barteit, S.: The impact of wearable technologies in health research: Scoping review. JMIR MHealth UHealth **10**(1), e34384 (Jan 2022)
15. Lashkari, B., Musilek, P.: A comprehensive review of blockchain consensus mechanisms. IEEE Access **9**, 43620–43652 (2021). https://doi.org/10.1109/ACCESS.2021.3065880
16. Patil, R.M., Kulkarni, R.: Universal storage and analytical framework of health records using blockchain data from wearable data devices. In: 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). pp. 311–317 (2020). https://doi.org/10.1109/ICIMIA48430.2020.9074909
17. Popov, S.: Iota whitepaper v1.4.3. New Yorker **81**(8), 1–28 (2018)
18. Raji, R.: Smart networks for control. IEEE Spectrum **31**(6), 49–55 (1994). https://doi.org/10.1109/6.284793
19. Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., Vagneur, K., Zhang, B.: Distributed ledger technology systems: A conceptual framework. SSRN Electronic Journal (01 2018). https://doi.org/10.2139/ssrn.3230013
20. Rose, K., Eldridge, S., Chapin, L.: The internet of things: An overview. The internet society (ISOC) **80**, 1–50 (2015)
21. Sengupta, J., Ruj, S., Bit, S.D.: A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications **149**, 102481 (Jan 2020). https://doi.org/10.1016/j.jnca.2019.102481
22. Srivastava, G., Dwivedi, A.D., Singh, R.: Automated remote patient monitoring: Data sharing and privacy using blockchain (2018). https://doi.org/10.48550/ARXIV.1811.03417
23. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I., Mazura, M., Harrison, M., Eisenhauer, M., Doody, P.: Internet of things strategic research roadmap (01 2009)
24. Voulgaris, S., Fotiou, N., Siris, V.A., Polyzos, G.C., Jaatinen, M., Oikonomidis, Y.: Blockchain technology for intelligent environments. Future Internet **11**(10) (2019). https://doi.org/10.3390/fi11100213
25. Wang, X., Zha, X., Ni, W., Liu, R.P., Guo, Y.J., Niu, X., Zheng, K.: Survey on blockchain for internet of things. Comput. Commun. **136**, 10–29 (2019)
26. Xie, Y., Lu, L., Gao, F., jiang He, S., juan Zhao, H., Fang, Y., ming Yang, J., An, Y., wei Ye, Z., Dong, Z.: Integration of artificial intelligence, blockchain, and wearable technology for chronic disease management: A new paradigm in smart healthcare. Current Medical Science **41**(6), 1123–1133 (Dec 2021). https://doi.org/10.1007/s11596-021-2485-0
27. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE international conference on software architecture (ICSA). pp. 243–252. IEEE (2017)