Wireless Networks (2024) 30:6507–6521
https://doi.org/10.1007/s11276-023-03458-7

Phonendo: a platform for publishing wearable data on distributed ledger technologies

Francisco Moya[1] · Francisco J. Quesada[1] · Luis Martínez[1] · Fco Javier Estrella[1]

Accepted: 13 July 2023 / Published online: 7 August 2023

Abstract
Nowadays, Internet of Things (IoT) devices, especially wearable devices, are commonly integrated into modern intelligent healthcare software. These devices enable medical practitioners to monitor pervasively patients' parameters outside the clinical environment. However, the ease of manipulating wearable devices and their data streams raises concerns regarding patient privacy and data trust. Distributed ledger technologies (DLT) offer solutions to enhance resistance against information manipulation and eliminate single points of failure. By leaveraging DLT, wearable-based solutions can be developed with a wider range of capabilities. This paper carries out an analysis of shortcomings, limitations, potential applications and needs in the medical domain, to introduce Phonendo 1.0, a DLT–IoT-based platform designed to capture data streams from wearable devices and publishing them on a distributed ledger technology infrastructure. The architecture and its difference services are justified based on the identified needs and challenges in the medical domain.

Keywords Internet of Things · Distributed ledger technologies · Telemedicine

1 Introduction

In the medical domain, novel intelligent computing services usually leverage wearable and IoT devices to address various health and well-being issues [2, 38]. Nowadays, there is a wide diversity of available devices, sensors, and computer-based solutions that fall under the category of IoT. However, defining IoT is not straightforward, and multiple definitions can be found in the specialised literature [20, 62, 67]. These definitions attempt to delimit IoT based on the characteristics of its elements [67], communication typology [62], enabling aspects for applications [66] or even from a temporal perspective that considers the ratio of connected objects to the internet versus people [24]. In our proposal, we focus on the use of wearable devices, which are considered a subset of IoT devices according to Rose et al. [67].

The IoT has evolved into a robust and demanded service infrastructure for the healthcare sector, known as the Internet of Medical Things (IoMT) [65]. Similarly, the term *mHealth* is used to describe the utilisation of mobile devices and other wireless devices in healthcare [13, 54]. Wearable devices enable pervasive remote monitoring of patient's parameters such as heart rate, body temperature, cardiovascular pressure or glucose levels among others. Therefore, wearables are highly suitable for implementing IoT-based solutions in the health and well-being domains [38]. Thus, the gathered data streams related to these parameters can be used to recognise complex activities such as physical exercise, sleep cycles, anxiety episodes, cardiac crises or loss of consciousness [18].

Despite the relevant features and advantages provided by wearable devices for health-based solutions, it should be noted that IoT devices in general and wearables in particular, suffer from security problems [81]. These issues have resulted in the failure of many real-world related proposals [49, 75] and impede the current and future development of promising health services based on these devices. In fact,

✉ Francisco J. Quesada
fqreal@ujaen.es

Francisco Moya
fpmoya@ujaen.es

Luis Martínez
martin@ujaen.es

Fco Javier Estrella
estrella@ujaen.es

[1] Universidad de Jaén, Jaén, Spain

complex analysis of wearable data streams can lead to the discovery of critical data [25, 41].

Consequently, in order to address these security problems, recent proposals explore the use of DLT to leverage its features [26, 80]. Specifically, the promise of resistance to information tampering and the resilience to single points of failure, which alleviate existing security concerns. Addressing these security challenges is crucial to enhance the comprehensive context of patient's clinical information and other data elements included in precision medicine [37]. Thus, the combination of IoT and DLTs represents a significant advancement in medical applications such as [35, 64]: drug traceability, patient monitoring/electronic health records, and managing medical records.

Following such a trend, this paper aims to study the applicability of DLTs to a real-world wearable scenario, with a primary focus on securing the processes of collecting, storing and publishing health wearable data. Consequently, an analysis of shortcomings, limitations, potential applications and needs in the medical domain is conducted based on the specialised literature, to introduce a novel proposal for secure IoMT based on DLT and to develop a platform so-called *Phonendo*. Phonendo enables the pairing of wearable devices, capturing and verifying their data streams, and publishing them on a dedicated DLT infrastructure, commonly referred as DLTI, thus avoiding previous flaws.

The remaining of the contribution is structured as follows. In Sect. 2 related works are analysed to extract the key features for developing a DLT-based framework. Section 3 includes an analysis of the impact of publishing data on a DLTI, their adaptation to a wearable scenario and the potential benefits and limitations of using DLTs in the medical domain, introducing some possible applications. Section 4 presents the architecture of Phonendo and justifies its design decisions. The paper finishes with the conclusions and future work, included in Sect. 5. Appendix reviews the main concepts of IoT and DLT necessary for a clear understanding of the proposal.

2 Related works

The need for IoT solutions to benefit from certain DLT characteristics, has resulted in the integration of DLT in these solutions [7]. The basic concepts about IoT and DLT are provided in Appendix for reference, if needed.

Since Samaniego et al. proposed the idea of Blockchain as a Service (BassS) for IoT [69] dozens of researchers have applied DLT to their work [7, 57, 77]. Multiple examples can be found in the literature across various contexts. For example, in the industry, for industrial IoT solutions [11, 27], such as those focusing on supply chain [85], or food traceability [47]. Athavale et al. integrate blockchain with IoT for storing and managing data [9], and similarly, Ozyilmaz et al. take advantage of smart contracts to develop a marketplace for data obtained by IoT devices [56].

Apart from the various applications in different scenarios, most works focus on using DLT, generally blockchain, as a security mechanism for their systems [29, 60]. It is notably used for forensics [45, 48] and access control [36, 58].

In the medical domain, nowadays, more and more medical practitioners are encouraging patients to use wearable devices to collect medical records outside the hospital environment. Patients are willing to do so as they want to be involved in their diagnosis and make more informed decisions about their health [6]. However, the increasing number of wearable medical devices has raised concerns about the possibility of these devices being hacked by unauthorised individuals to access patients' health records [4]. These are the main issues that have motivated the adoption of DLT in the medical domain.

It is necessary to highlight that most of proposed solutions are still prototypes and not yet in use. However, as DLTs mature, they will be increasingly adopted in real scenarios. Gupta el at. proposed a blockchain-based framework for telesurgery using Hyperledger Fabric (HF) [33]. Alam et al. proposed a framework that integrates blockchain and IoT to enable data sharing for remote patient monitoring, aiming to provide accurate diagnosis while reducing costs and unnecessarily hospitalisations [6]. In this case, blockchain is mainly used to foster transparency and information exchange between parties. Similarly, Amofa el at. introduce a prototype that takes advantage of Smart Contracts (SCs) to securely share personal health data [8].

More recently, Namasudra et al. proposed the use of Ethereum and SC for generating and verifying medical certificates [51], while Khan et al. store and update information obtained from a brain-computer interface in HF using SCs [42].

Regarding the storage of electronic health records, Shahnaz et al. use Ethereum to provide a secure storage for electronic health records by implementing multiple access rules via SCs [73].

To sum up, those permissionless solutions that uses Ethereum offer transparency and can benefit from SC, but have associated transaction fees. Moreover, these solutions do not scale well and transactions are confirmed with a delay of seconds.

On the other hand, permissioned approaches, mostly based on HF, scale well and transactions are confirmed quickly. However, the existence of a central authority to provide access to participants, can be seen as a lack of transparency.

To address these issues, researchers have turned to IOTA (see "Appendix"), leveraging its unique features as permissionless DLTI that offers high scalability and fee-less transactions. Several studies have explored the use of IOTA in the healthcare domain. For instance, Cisneros et al. proposed CoviReader, a decentralised healthcare management system that anonymously share user data to assist in controlling the spread of Covid-19 [21]. Abdullah et al. utilised IOTA MAM channels to ensure secure data sharing within a healthcare system [3]. Rydningen et al. highlighted the advantages and opportunities of using IOTA for health data management, while also discussing concerns such as privacy, security, or data inaccuracies [68].

Given the aforementioned considerations and recognising the benefits of IOTA, this paper introduces *Phonendo*, a platform that leverages IOTA as its chosen DLTI (see Sect. 4).

3 Examining the feasibility of DLT in mHealth scenarios

In this section, it is analysed the impact of publishing data on a DLTI, their adaptation to a wearable scenario, as well as the potential applications and limitations.

3.1 Analysis of the impact of a DLTI on the data register

Before designing or implementing any solution that integrates a DLTI, it is essential to conduct and analysis. This analysis becomes even more important in IoT scenarios because the suitability of DLTI depends on the characteristics of each environment (e.g. number of devices, type of data, data frequency...), being necessary to justify the convenience of using a DLTI. In our analysis, we consider the following aspects: decentralisation, confidentiality, performance, and transparency.

Regarding decentralisation, we should evaluate whether our system benefits from the absence of a central authority controlling and validating transactions. In mHealth scenarios, decentralisation may be beneficial, as it allows patient data to be validated and stored in a more secure and transparent manner, without the need for a central authority. Therefore, these systems might benefit from being decentralised.

Concerning confidentiality, we should consider whether replicating data in multiple nodes violates any restrictions. It is important to emphasise, that all data stored in a DLTI is immutable, so no sensitive data should be stored in it. Therefore, DLTIs are only suitable in mHealth, if the solution only stores anonymous data.

In terms of performance, a traditional database outperforms a DLTI in managing large volumes of data and numerous writing operations. Additionally, it is necessary to determine the maximum delay that our processes can tolerate until a piece of data is stored. For example, in emergency response systems, data must be stored immediately, while in a smart home, it might be acceptable if data are stored within a few seconds. Considering that most IoMT solutions involve sending recurrent but small data messages, DLTIs are recommended in mHealth solutions as long as the selected DLTI has high scalability and the solutions can accommodate its transaction time.[1]

Regarding transparency, DLTIs cannot remove nor modify previous transaction, preserving dependencies between them, which is crucial to have traceability within the records. This allows third parties to audit the stored data, providing transparency to the process. For example, mHealth can benefit from this traceability to recognise health events from patients' vital signs.

In summary, after considering the above aspects we conclude that DLTIs are suitable for use in mHealth scenarios. Therefore, any solution that uses data stored on a DLTI can benefit from: (i) resilience to single points of failure, (ii) resistance to alteration and/or deletion of data, (iii) protection timestamp modification, and (iv) resistance to identity spoofing [19].

Feature (i) is provided by the use of a distributed system rather than a centralised one. Hence, compromising the entire system would require attacking multiple nodes. Due to the fact that, in a distributed system where there is no central authority verifying the network status, consensus mechanisms are integrated to carry out the verification process. These mechanisms make DLTIs tamper-proof, preventing users from rewriting the ledger. This fact, provides features (ii) and (iii) to the stored data. Finally, feature (iv) is provided by the use of asymmetric cryptographic mechanisms, such as digital signatures.

From other perspective, it is also important to analyse the impact of DLTIs that support SCs, allowing the development of decentralised applications (dApps) because they enable: (i) implementation of crypto-economic models as a way to incentive users to share data (e.g. geolocation); (ii) allocation of non-fungible tokens to prove participation in the system; (iii) marketplaces for buying and selling aggregated or individual data; or (iv) Decentralised Autonomous Organisations (DAOs) [44] to regulate aspects such as adding permissions or issuing rewards to participants.

At this point, we have only focused on storing data on a DLTI ledger. However, in some cases, using a Distributed File System (DFS) such as InterPlanetary File System

[1] The *transaction time* is the time for confirming value transactions.

Table 1 Comparison table between the DLT

	Ethereum	HF	IOTA
Type	Permissionless	Permissioned	Permissionless
Topology	Blockchain	Blockchain	Direct acyclic graph (DAG)
Consensus	Proof of stake (PoS)	Practical byzantine fault tolerance (PBFT)	Fast probabilistic consensus (FPC)
Scalability	Low	High	High
Support to SC	√	√	√
Cost	Fee	Feeless	Feeless

(IPFS)[2] could be sufficient. Rather than storing a file in a single, centralised location, it is disseminated across a distributed system of users, each holding a portion of the overall data. Nonetheless, it is necessary to highlight that a DFS might either: (i) lose some of the benefits offered by a DLTI or (ii) require additional actions to achieve equivalent characteristics.

For example, using a DFS will simplify both the generation of multiple values for a single read and information concealing to deliver a particular value. Apart from that, solutions such as IPFS do not guarantee specific value retrieval, requiring the existence of nodes with a copy of that particular value. Thus, own nodes or dedicated services must be used to prevent data loss.

3.2 Adapting to a mHealth wearable scenario

Focusing on a mHealth scenario with a prominent use of wearables, it is necessary to figure out how can we adapt the architecture to such devices and determine which DLTI is the most appropriate for storing their data.

Adapting the architecture to wearable devices

A platform that exposes an architecture adapted to wearables must take into consideration their characteristics. The main ones are: (i) concurrency of multiple devices, (ii) small data payloads, (iii) recurrent data capture, (iv) sensitive data, (v) easy attackability, (vi) low computational resources, (vii) different hardware specifications, and (viii) different communication protocols.

Characteristics (i), (ii), (ii), (iv) have been previously considered in Sect. 3.1 regarding decentralisation, performance and confidentiality. Thus, the architecture of wearable devices should have high scalability to allow processing multiple devices continuously sending small, but recurrent messages. Moreover, only anonymous data should be published on a DLTI. Regarding (V), security mechanisms need to be implemented to maintain system integrity and data privacy even if a given wearable is hacked. These mechanisms cannot require wearables to carry out extra computational costs, concerning (Vi). Finally, considering characteristics (Vii) and (Viii), the architecture should address the interoperability issues caused by heterogeneous hardware and communication protocols.

Selection of the most appropriate DLTI

In our scenario, the main consideration when choosing a DLTI may focus on whether to select a permissioned or a permissionless DLTI. On the one hand, the former optimises computational resources, reduces operating costs and increases control over access to information. On the other hand, the latter allows any entity to verify the information within the ledger and build third-party applications using these data.

Therefore, we consider that a permissionless DLTI would allow a larger number of applications to be conceptualised and thus, our proposal focuses on this type of DLTIs.

Considering the different DLTI options, described in Table 1, IOTA [59] has been chosen as the DLTI for our platform. It is, a DAG-based DLTI that has the following features DLTIs [28]:

- *No commission costs on writing* IOTA is feeless, so users do not have to pay to publish on the Tangle. Therefore, no tokens are required for the publication process.
- *Low latency information addiction* In IOTA, there are no blocks. Any new transaction needs to validate two previous transactions in order to be appended in the ledger. This gives the infrastructure a great throughput.
- *Libraries* The IOTA ecosystem provides multiple libraries that facilitate the integration of applications with the DLTI.
- *Support for SC* The latest version of IOTA integrates the IOTA Smart Contract Protocol (ISCP), allowing developers to use SC in the DLTI.

To sum up, IOTA is a highly suitable DLTI for our platform in terms of efficiency and performance. Nonetheless, there are two significant issues that need to be considered. Firstly, due to its feeless nature, the ledger quickly

[2] https://ipfs.io/.

increases in size. To address this issue, a process of instantiating a new ledger and a balance snapshot are periodically performed. Moreover, a *Permanode* [28] is required to retrieve historical information. Secondly, IOTA requires Proof of Work (PoW) per transaction as a SPAM prevention mechanism. Thus, if the publishing device has limited computational resources, it may delegate the PoW to a third party.

It is important to note that both problems arise from the use of IOTA's public network and not from the use of its technology. Therefore, it would be possible to deploy a hypothetical DLTI using its technology and limit itself to storing information of interest to the domain while reducing or eliminating the PoW per transaction. However, it is easy to reason that (i) if access is not limited, this hypothetical DLTI could be easily attacked, whereas (ii) if access is limited, we are essentially converting the DLTI in a permissioned one.

3.3 Potential applications and limitations of solutions

After analysing the impact of a DLTI on the data register and the considerations needed to adapt to a wearable scenario, it is necessary to point out both potential applications and limitations.

Regarding the former, our hypothesis is that having a platform with the characteristics mentioned in Sect. 3.1 allows for the conceptualisation of applications that can benefit from the value added by this platform, especially in healthcare:

- *Validation of medical studies* It is possible to guarantee that the data have not been manipulated and reflect the one captured in the given study.
- *Transparency and traceability* The platform enables determining the time when a healthcare episode begins, avoiding its concealment. This information can be used to measure aspects such as the reaction time of health services or identify the source of the episode, thereby preventing negligence.
- *Health research* With data stored in the platform from trusted sources, "high-quality" data can be provided for studies, where quality refers to the veracity of the available data.
- *Certification of medical conditions* Controlled environments can be used to perform activities such as such as stress tests on elite athletes and certify the result to a third party.
- *Incentivising the performance of healthy activities* Gamification systems can be established to incentivise healthy habits among citizens, with the involvement of governments and health practitioners.
- *Information sharing between different entities* Users can share their health records with different specialists.

However, it is important to note that any of the features listed in Sect. 3.2 can be defeated by employing different attacks.[3] Therefore, it is necessary to highlight that a data-driven solution should not be built if the cost of attacking it is lower than the potential benefit.

Furthermore, any solution focused on capturing data should be reconsidered if participants have to provide data that may benefit or harm them. This is because such scenarios can motivate participants to misbehave in order to obtain benefits. This is particularly important if the data can be manipulated prior to publication.

Finally, considering the sensitiveness of data captured by wearables, solutions should be avoided if users' privacy is at risk, even if the information can be encrypted prior to storage.[4]

Note that the mentioned limitations not only apply to the proposed platform, but also to any platform with similar characteristics. Therefore, solutions should be ideally implemented in those scenarios that meet one or more of the following characteristics:

- Individuals have no 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 captured do not cause harm 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

In previous sections we analysed the importance of DLTIs for storing data from IoT devices and identified IOTA as the most suitable DLTI. We also explored the different potential applications of this infrastructure in *mHealth*.

Therefore, in this section, we present *Phonendo*, a platform consisting of several software services that manages the entire data lifecycle from wearable device data collection to publishing them on IOTA. This section describes Phonendo's architecture, services, design

[3] 51% attacks on certain DLTIs for (vi) and (ii), social engineering attacks for (iii), or denial of service attacks for (iv).

[4] It is necessary to highlight that if we store data in a DLTI, encryption is not enough because the data will be permanently stored and encryption algorithms might be cracked in the future, revealing all sensitive data.

considerations and data flow; which will be further detailed in the coming subsections. Phonendo's source code is available on GitHub.[5]

4.1 Phonendo's architecture

Phonendo's architecture follows a microservice event-driven approach and it is comprised of five components: *Reader*, *Manager*, *Storage*, *Verifier* and *Publisher*. Figure 1 illustrates the interconnections between all the components (see Sect. 4.2) and their main functionalities. This architecture has been designed considering flexibility, scalability and adaptability to different applications.

Comparing Phonendo's architecture with other proposed DLT-based architectures for healthcare, we observe that all proposals share modules for collecting and storing information. For instance, Casado-Vara and Corchado propose three layers dedicated to data collection, management, and storage [17]. Leeming et al. propose a blockchain layer and a storage layer with a blockchain-agnostic design [46]. Abdullah et al. propose an architecture focused on storage and information retrieval, distinguishing between *publishers*, who send information to IOTA, and *fetchers*, who read information from IOTA [3]. In our case, in addition to these common modules ("*Reader", "Manager", "Storage*", and "*Publisher*"), we introduce the "*Verifier*", which is responsible for ensuring the integrity and authenticity of the data.

The current implementation of Phonendo represents our initial efforts to validate the end-to-end functionality of the platform. Our primary objective was to demonstrate the operational feasibility of Phonendo by seamlessly integrating wearable device data.[6]

For the development of Phonendo, we selected the Node.js framework and JavaScript programming language due to their suitability for rapid prototyping and their widespread adoption within the developer community. The choice of HTTP as the communication protocol was driven by the simplicity it offers in facilitating data transfer between services.

During the implementation phase, we utilised the *Pine Time*[7] smartwatch as a reference device to ensure compatibility and assess the integration of Phonendo with a real-world wearable device. This allowed us to validate the functionality of the platform and its ability to handle data from smartwatches, which are commonly used in healthcare and fitness applications.

It is important to note that the current implementation of Phonendo serves as a starting point for further research and development. As we continue to refine the platform and explore additional use cases, we anticipate introducing enhancements and optimisations based on empirical experimentation and user feedback.

4.2 Phonendo's services

In this section, the services that constitute Phonendo's architecture are described. These services are designed to handle different aspects of the data lifecycle and enable the seamless flow of data within the platform. Below, we provide an overview of each service:

- *Reader*: It manages the connection with the wearables, acting as the gateway of the system. When a new data is received, a verification process is carried out to verify the sender. If it was previously registered in Phonendo, the event is sent to *Manager* to start the process, otherwise, the new sender is registered in the platform.
- *Manager*: It manages the life cycle of the data interconnecting all Phonendo's services. It main responsibilities are (i) encapsulating communication and orchestrating with the rest of components to perform the business logic and (ii) certifying data and data provenance. To do so, each message is signed with a wearable's public/private key. This key is generated for each wearable device using its MAC address and a given password, applying *SHA256* algorithm [31]. This password is owned by *Manager* and unique on each application.
- *Storage*: It enables both modelling information and controlling the state of data in the operational flow. It allows retrying any potential event that has not been sent due to an infrastructure/software failure. To improve the platform's performance and scalability, key-value storage database engine has been used *LevelDB*.[8]
- *Verifier*: It validates the integrity of the data using multiple heuristics, generating as a result of its execution a signed message that timestamps the captured data. Those heuristics may be different depending on the scenario, but in our case, *Verifier* checks if values are within allowed ranges; and data timestamps to avoid old transactions.
- *Publisher*: It is responsible to carry out the publication on the IOTA network [28] where the messages signed by *Verifier* are published. In order to allow traceability a common index has been set. In addition, each message

[5] https://github.com/sinbad2-ujaen/phonendo.

[6] https://github.com/sinbad2-ujaen/phonendo/tree/main/demo provides demonstrations of the end-to-end functionality of the system.

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

[8] https://github.com/google/leveldb.

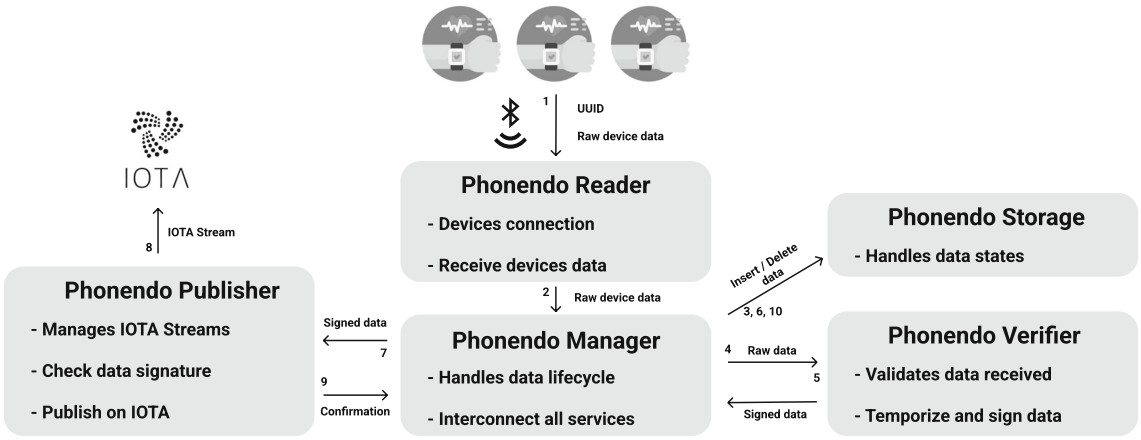


Fig. 1 Phonendo architecture

is linked to the last *messageId* as the parent message, and as future improvement.

4.3 Architectural advantages of the phonendo platform

The design of Phonendo's architecture is the result of careful considerations to meet the requirements of a robust and flexible platform for managing wearable device data. To achieve this, Phonendo adopts a microservice event-driven architecture, which offers several advantages. Let's delve into the reasons for each component and the benefits they bring to the platform:

- *Reader*: The Reader is specifically designed to support various types of wearables and establish a secure and reliable communication channel. One of the key advantages of separating the Reader functionality is its low computational requirements, allowing it to run on low-spec devices. This opens up the possibility of deploying multiple Reader instances at a low cost, both in terms of energy consumption and acquisition. Additionally, the use of low-power devices enables battery-powered operation, further enhancing the scalability and flexibility of the Phonendo platform.
- *Manager*: The Manager service serves as the orchestration layer in Phonendo's architecture. It plays a crucial role in managing system changes and addressing various challenges that may arise. By separating the Manager component, Phonendo ensures the flexibility to adapt to evolving requirements and seamlessly handle issues.

  One important aspect of the Manager is its role as the representative of the Reader components. While Readers capture data from wearable devices, it is the Manager that generates and manages the private/public key pairs for each device, as well as handles the communication process. This design ensures the Manager's authenticity and prevents unauthorised entities from impersonating it.
- *Storage*: The Storage service in Phonendo is a vital component responsible for managing data and controlling its state throughout the operational flow. By separating the storage functionality, Phonendo offers several advantages. Firstly, it enables the Manager to operate with stateless logic, allowing for streamlined data orchestration and ensuring data integrity. In addition, the Storage service provides resilience in case of Manager failures or downtime by allowing the Manager to consult the stored data and reconstruct the system's state.

  Moreover, the separation of the Storage service opens up possibilities for further enhancements. For instance, Phonendo can explore distributing information across multiple Storage services, enabling efficient data processing and resource utilisation. Additionally, the platform can leverage the flexibility of the Storage service to accommodate different database technologies, providing the freedom to switch to alternative solutions based on specific needs and scalability requirements.

  Furthermore, the Storage service can serve multiple Managers, enabling centralised data storage and retrieval while maintaining modularity and scalability. This capability empowers Phonendo to support diverse use cases and scenarios where multiple Managers can access and interact with the same storage infrastructure.
- *Verifier*: The Verifier service in Phonendo plays a critical role in ensuring data integrity and authenticity. While its primary function is to validate the received data, it goes beyond that by issuing a verifiable

signature on the verified information. This signature serves as proof of the Verifier's endorsement, adding an additional layer of trust and establishing the Verifier as a trusted authority.

The separation of the Verifier from the Manager in Phonendo's architecture has several motivations and potential future implications. By isolating the Verifier, Phonendo enables it to operate independently, allowing for enhanced security and trust. One possible avenue for future exploration is the publication of the Verifier's public key on a trusted platform, such as a blockchain, along with associated metadata. This would facilitate the establishment of hierarchical trust endorsements, where higher-level Verifiers endorse the identity and verification capabilities of lower-level Verifiers.

Furthermore, the use of advanced governance frameworks could enable the endorsement of trust from trusted entities, such as notaries or regulatory bodies, to specific Verifiers within the Phonendo ecosystem. These endorsements could enhance the overall trustworthiness and reliability of the verified data. Additionally, the exploration of revocation mechanisms could allow for the timely and secure revocation of certain data, ensuring data accuracy and accountability.

While these ideas are still in the realm of future possibilities, they serve as motivations for the architectural decision to separate the Verifier from the Manager in Phonendo.

- *Publisher*: The Publisher service in Phonendo is responsible for data publication on the IOTA network. By separating this functionality, Phonendo achieves flexibility in resource allocation and scalability. Lightweight devices like Arduino or Raspberry Pi can be utilised for the Reader components, while more powerful devices can handle the Publisher service. This design choice enables cost-effective deployment and horizontal scaling.

  Furthermore, the separation of the Publisher service opens up possibilities for future enhancements. Alternative DLTs can be seamlessly integrated into Phonendo, providing adaptability to evolving healthcare data management requirements. Additionally, exploring collaborative PoW schemes and hybrid data publication approaches can optimise efficiency and security.

The architecture of Phonendo is designed with the principles of simplicity, performance, flexibility, and scalability in mind. By separating the functionality into individual services, Phonendo provides a modular and adaptable platform that can be easily tailored to different application scenarios. This design approach empowers developers and researchers to integrate their IoT solutions with a DLTI effectively.

4.4 Phonendo's data flow

This section describes the data flow carried out in Phonendo and the interaction of all its services detailed above (see Fig. 2).

1. *Matching* It is the first step to allow the connection between a wearable device and Phonendo. The connection process is managed by the *Reader* component. *Reader* performs some basic verifications associated with a minimum contract, indicating its serial number, the type of wearable device, data types, and other basic information. Finally, it is registered in the database and provides an API token to perform the rest of the operatives.

```
{
    "device":"F5:C5:D8:50:BB:D5",
    "type":"SMARTWATCH",
    "serialNumber": 234324875123213,
    "creationDatetime": 1676389938
}
```

2. *Data reception* Once a device is successfully registered it can start sending events to the system. This step involves *Reader* and *Manager* components. *Reader* notifies *Manager* when new data is received through a HTTP request. Once *Manager* receives data, it is involved in data processing, verification and publication.

```
{
    "type": "HEART_RATE",
    "value": 100,
    "device": "F5:C5:D8:50:BB:D5",
    "creationDatetime": 1676846304009,
}
```

3. *Data processing*. *Manager* requests *Storage* to model the data to allow abstraction, obtaining as a result a JSON document. Internally, *Storage* stores these data and sets its status to "*Captured*".

```
{
    "key": "9dc49539-68c4-4ef4-b7b6-d7c25dbb40c9",
    "value": {
        ...
        "status": "Captured"
    }
}
```

4. *Verification*. *Manager* signs the data to ensure data provenance. In addition, *Manager* requests *Verifier* to verify and sign this document, resulting in a signed JSON document. Data is signed using the *Verifier*'s public/private key and SHA256 algorithm. This key is shared between all the instances in the deployed environment.

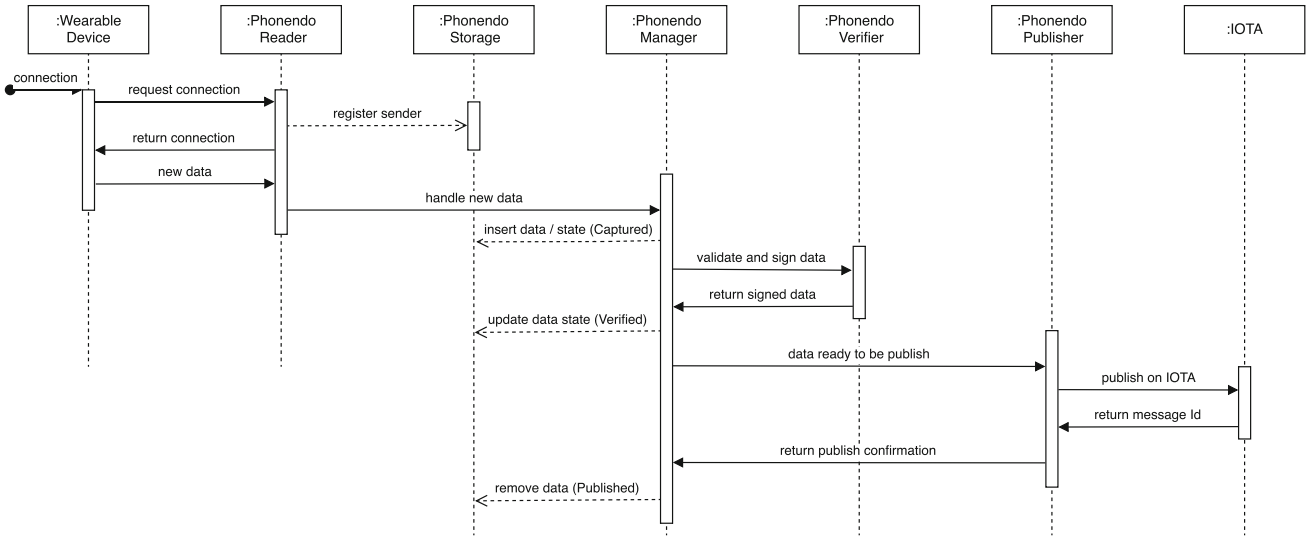


Fig. 2 Phonendo's sequence diagram

```
{
    "key": "9dc49539-68c4-4ef4-b7b6-d7c25dbb40c9",
    "value": {
        ...
        "managerSign": "303f021d437791d6442dd0f8309...",
        "managerSignDatetime": 1676846304009,
        "verifierSign": "303f021d48885442d6442dd0f8309...",
        "verifierSignDatetime": 1676846304010,
    }
}
```

5. *Status update: verified*. *Manager* notifies *Storage* the data verification, and *Storage* updates the status to "*Verified*".

```
{
    "key": "9dc49539-68c4-4ef4-b7b6-d7c25dbb40c9",
    "value": {
        ...
        "status": "Verified",
        ...
    }
}
```

6. *Data publication Manager* requests the publication by *Publisher*. This process involves data preparation, to create the IOTA message structure and send it to the Tangle. Obtaining, as a result, the confirmation of the publication in IOTA with the "*messageId*".

```
{
  "message": {
    "networkId": "6514788332515804015",
    ...
  "messageId": "b19e2da6e4ca4dc822cc8b13d...."
}
```

7. *Status update: published*. *Manager* notifies *Storage* of the publication, which performs the removal from the database to end the data lifecycle.

This data flow ensures the seamless processing and publication of wearable device data in Phonendo, providing a reliable and secure platform for managing and utilising such data.

5 Conclusions and future work

In this paper, we have introduced a novel proposal for securing IoMT based on DLT and developed a platform called Phonendo that allows for pairing wearable devices, capturing, verifying, storing their data streams and publishing them on a dedicated DLTI, thus avoiding previous flaws. Namely, Phonendo (version 1.0) has been presented describing its architecture, services and data flow. Its code and end-to-end demos are publicly available on GitHub, therefore, developers and researchers can take advantage of Phonendo to integrate their IoT solutions with a DLTI.

Currently, Phonendo is limited to the Bluetooth Low Energy (BLE), so devices with other communication protocols are not compatible. However, since Phonendo is open source and its code is available, any developer can extend the system to support new protocols and devices. It is important to note that Phonendo is a tool that researchers and practitioners can use as a starting point to develop trusted IoT systems adapted to specific scenarios.

Regarding future works, there are several directions that might be pursued. Phonendo's services can be extended as detailed in Sect. 4.3, by exploring different storage solutions; using advanced governance frameworks to provide trust; or optimising efficiency and security through collaborative PoW schemes and hybrid data publication. Additionally, the platform can be enhanced with more functionality, focusing on aspects such as encryption,

connection protocols, access regulation, query resolution or generation of analytical data. An example of such new features could be the integration of Self-Sovereign Identity (SSI), leveraging the *Identity* [28] framework provided by IOTA.

Appendix: Background

This appendix provides a brief overview of the basics concepts of IoT and DLT, which are essential for understanding our proposal.

Internet of Things

The recent advancement in communication, wireless sensor networks and information technologies have led to the development of systems that integrate numerous of devices to interact with their environments [12, 71, 83]. As a result, IoT has become a pervasive technology in people's daily lives, despite some reservations about its applicability in scenarios involving sensitive data such as, the health domain, due to various security issues [81].

Since its inception, IoT solutions have had a positive impact on various domain including transport and logistics [32, 84], smart environments [34, 78], social and personal applications [72], or healthcare [1, 10, 39].

However, most of IoT solutions face certain common challenges and limitations:

- *Massive amount of data and/or nodes*. IoT solutions typically integrate a large number of devices that continuously produce data. Managing and processing this massive amount of data is challenging, and ensuring data consistency between sensors can be even more difficult.
- *Decentralisation*. The presence of numerous nodes in an IoT network and their communication contribute to the decentralised nature of IoT [79].
- *Interoperability issues*. The heterogeneity of IoT devices usually results in the use of different communication protocols and software, leading to unstable and unpredictable connections.

The characteristics of IoT-based solutions and devices can give rise to various technological weaknesses and potential attacks on such applications [81]. Indeed, these attacks target vulnerabilities in different elements of the IoT solution including end devices, communication channels, network protocols, sensors, denial of service, and software.

To address these limitations, several authors have explored the potential of using DLTs [59, 70].

Distributed ledger technologies

The concept of DLT is built upon the principles of cryptography [61] and distributed database systems [55]. Cryptographic elements are employed to ensure data integrity and non-repudiation, while distributed database systems consist of a network of peers (nodes) where data is recorded without the involvement of any central authority. In recent years, DLTs have gained popularity due to their distinctive characteristics[63]:

- *Immutability*. Data stored in a DLTI is permanent and cannot be altered.
- *Decentralisation*. The network operates without central authority controlling it.
- *Distribution*. All network participants possess a copy of the records (ledger), ensuring complete transparency.
- *Tamper-proof*. As data cannot be modified, participants can trust the authenticity of the records within the network.
- *Time-stamped*. Each record is associated with a timestamp, which is valuable for traceability purposes.
- *Consensus*. The network implements mechanisms to determine its status through agreement among its participants.
- *Security*. Records are individually encrypted, and asymmetric cryptography is utilised, preventing participants from repudiating transactions carried out from their accounts.

Below are described the most popular types of DLTs: *blockchain* and *DAGs*.

Blockchain is the most prominent type of DLT, having been first used as Bitcoin's infrastructure to support Peer-to-Peer (P2P) economy [50]. In the blockchain, each transaction contains information about the sender, the recipient, and the transacted data [63]. Moreover, all transactions carried out in a certain time interval are stored in a *block*. Each block has an identifier that is the value resulted after computing a *hash* function of all block's content [23, 52].

A hash function is a one-way function that, given an input, produces a string of characters with a fixed length (*hash*). Thus, its two main particularities are that: (i) a minimum change in the input produces a significant change in the output, known as the "*avalanche effect*" [74]; and (ii) it is currently computationally challenging to get the input data from a given hash, unless the value is selected from a known pre-calculated domain.

Apart from the transactions, each block has the identifier of its previous block, which is also considered when computing the block's hash. This fact is what makes a chain of blocks. The first block, called the genesis block, has a previous block's hash that is essentially arbitrary,

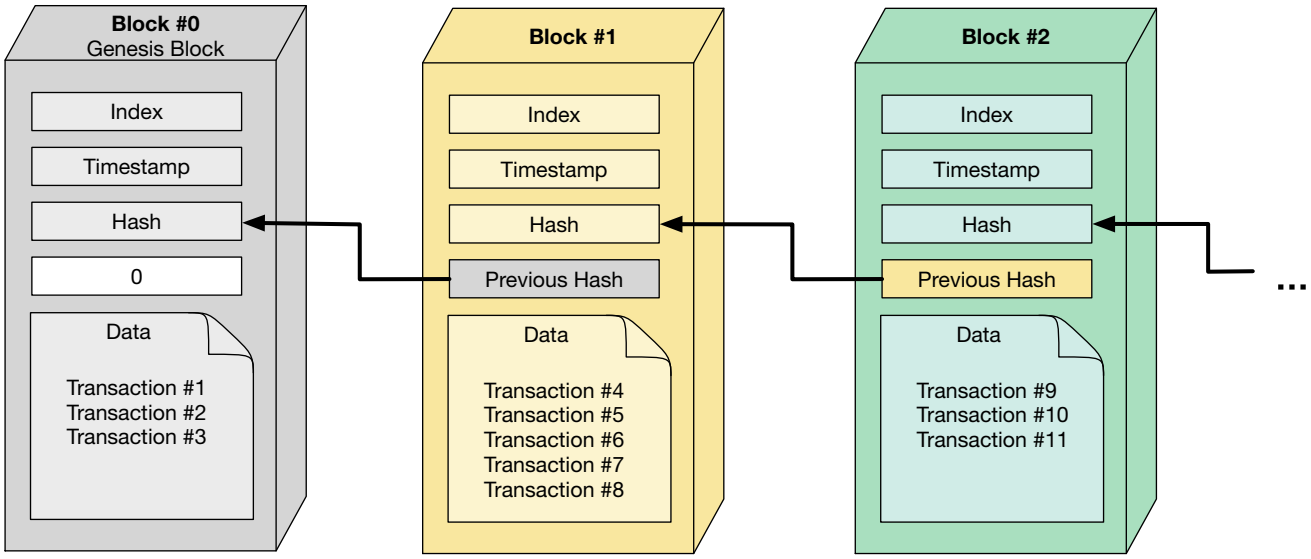
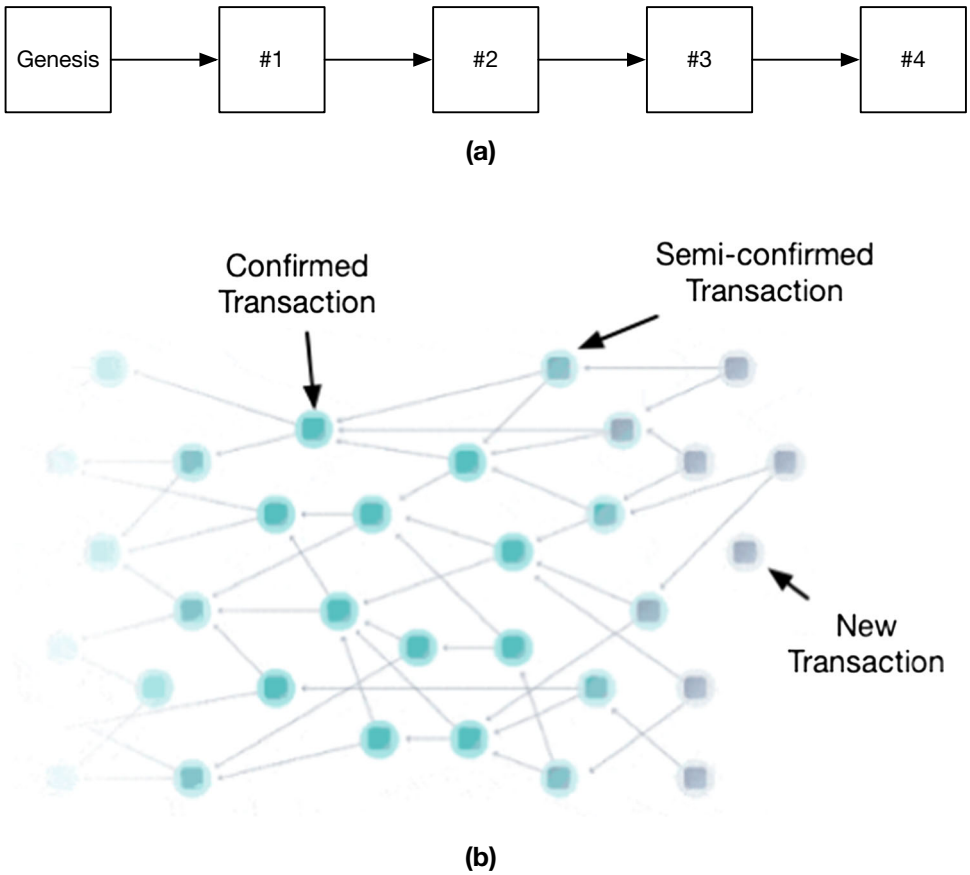


Fig. 3 Example of blockchain

Fig. 4 Example of DAG (IOTA tangle)



serving as the starting point for the blockchain. This can be a string of zeros, an empty string, or a predetermined seed, depending on the specific blockchain implementation.

Figure 3 depicts all the elements mentioned above.

Due to the fact that blockchain does not have a central authority that guarantees the network status (e.g. deciding which block should be appended to the chain), it is necessary to implement mechanisms that allow nodes to do so themselves. These mechanisms are the consensus

algorithms [82]. The two most used are [76]: PoW [30] and PoS [53].

Regarding user access, blockchains can be classified into: (i) *public*, where anyone can participate without restrictions; (ii) *private*, where data can be accessed only by users who are granted specific permissions; and (iii) *federated*, where there are pre-selected participants that are accepted. Each participant has an equal ability to influence network decisions, hence, this type of blockchain is not open to everyone but semi-private.

In 2015, the development of Ethereum [14] represented a technological shift for blockchain, from being exclusively used for electronic payments to the emergence of dApps [15]. dApps appeared thanks to the concept of SC which are pieces of code stored and executed on the blockchain [43] that fulfils an arrangement that involves an exchange of digital assets between two or more parties [40]. In this public blockchain, for each transaction and each new smart contract deployment, it is necessary to pay a fee in Ether (ETH) that is used to pay the computational cost associated with the transaction.

Despite the advancements brought by Ethereum, there are several scenarios where its application is not optimal, especially in cases where companies need to keep their valuable information private. This need is addressed by HF, the most representative federated blockchain [16]. In HF, the blockchain is formed by nodes of participating entities, requiring authorisation to join the network. Since HF does not necessitate miners to reach consensus, no transaction fees are incurred, leading to faster transaction processing compared to Ethereum [5]. It is important to note, however, that the choice between Ethereum and HF often hinges on the specific needs of the use-case. While certain HF frameworks allow executing Ethereum's audited smart contracts, the modularity and adaptability of HF can provide advantages when total control over a restricted domain is desired.

Although, blockchain is the most used DLT for public DLTIs, it still has several limitations such as limited throughput, transactions costs, confirmation delay or inequity [22]. The IOTA protocol was proposed in order to overcome these issues. Namely, IOTA aims at storing data from IoT devices in a ledger called "*the Tangle*", which uses a DAG [59].

The main advantages of IOTA are that it is public, feeless and scalable. The way in which a transaction is added to the Tangle is through a consensus algorithm that requires users to validate at least two transactions, previously sent to the Tangle, in order to complete their own IOTA transactions (see Fig. 4). The confirmation of a transaction is a complex process that involves network depth and acceptance percentage, among other factors.

The intricacies of the confirmation process are beyond the scope of this paper, but a detailed explanation can be found in the IOTA whitepaper [59].

Funding Funding for open access publishing: Universidad de Jaén/CBUA.

References

1. Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2021). Blockchain-assisted secured data management framework for health information analysis based on internet of medical things. *Personal and Ubiquitous Computing*, (pp. 1–14).
2. Abboushi, B., Safranek, S., Rodriguez-Feo Bermudez, E., Pratoomratana, S., Chen, Y., Poplawski, M., & Davis, R. (2022). 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*. https://doi.org/10.3389/fbuil.2022.787289.
3. Abdullah, S., Arshad, J., Khan, M. M., Alazab, M., & Salah, K. (2022). Prised tangle: A privacy-aware framework for smart healthcare data sharing using iota tangle. *Complex & Intelligent Systems*, pp. 1–19.
4. Agbo, C. C., & Mahmoud, Q. H. (2019). Comparison of blockchain frameworks for healthcare applications. *Internet Technology Letters, 2*(5), e122.
5. Aggarwal, S., & Kumar, N. (2021). Hyperledger. In *Advances in computers*, (vol. 121, pp. 323–343). Elsevier.
6. Alam, T. (2020). mhealth communication framework using blockchain and iot technologies. *International Journal of Scientific & Technology Research, 9*(6).
7. Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the Internet of Things (IoT): A systematic literature review. *Sensors, 22*(4), 1304.
8. Amofa, S., Sifah, E. B., Kwame, O., Abla, S., Xia, Q., Gee, J. C., & Gao, J. (2018). A blockchain-based architecture framework for secure sharing of personal health data. In *2018 IEEE 20th international conference on e-Health networking, applications and services (Healthcom)*. (pp. 1–6). IEEE.
9. Athavale, V. A., Bansal, A., Nalajala, S., & Aurelia, S. (2020). Integration of blockchain and IoT for data storage and management. *Materials Today: Proceedings*.
10. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

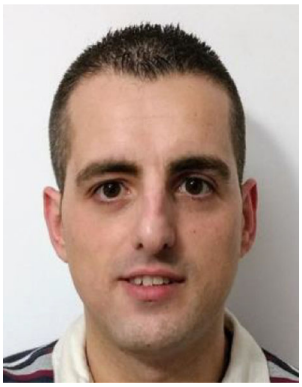
11. Bai, L., Hu, M., Liu, M., & Wang, J. (2019). BPIIoT: A light-weighted blockchain-based platform for industrial IoT. *IEEE Access, 7*, 58381–58393.
12. Bail, R., Kovaleski, J. L., da Silva, V. L., Pagani, R. N., & Chiroli, D. M. (2021). Internet of things in disaster management: Technologies and uses. *Environmental Hazards, 20*(5), 493–513.
13. Birkmeyer, S., Wirtz, B. W., & Langer, P. F. (2021). Determinants of mhealth success: An empirical investigation of the user perspective. *International Journal of Information Management, 59*, 102351.
14. Buterin, V. (2013). Ethereum. *White Paper*, *1*, 22–23.
15. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper, 3*(37), 2–1.
16. Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers*, (vol. 310, pp. 1–4). Chicago, IL.
17. Casado-Vara, R., & Corchado, J. (2019). Distributed e-health wide-world accounting ledger via blockchain. *Journal of Intelligent & Fuzzy Systems, 36*(3), 2381–2386.
18. Chen, L., Hoey, J., Nugent, C. D., Cook, D. J., & Yu, Z. (2012). Sensor-based activity recognition. *IEEE Transactions on Systems , Man, and Cybernetics, Part C (Applications and Reviews), 42*(6), 790–808. https://doi.org/10.1109/TSMCC.2012.2198883
19. Chen, Y., Trappe, W., & Martin, R. P. (2007). Detecting and localizing wireless spoofing attacks. In *2007 4th Annual IEEE Communications Society Conference on sensor, mesh and ad hoc communications and networks*. (pp. 193–202). IEEE.
20. chetansharma.com: Correcting the iot history, http://www.chetansharma.com/correcting-the-iot-history/. Last accessed 24 Jan 2023.
21. Cisneros, B., Ye, J., Park, C. H., & Kim, Y. (2021). Covireader: Using iota and QR code technology to control epidemic diseases across the us. In *2021 IEEE 11th annual computing and communication workshop and conference (CCWC)*. (pp. 0610–0618). IEEE.
22. Conti, M., Kumar, G., Nerurkar, P., Saha, R., & Vigneri, L. (2022). A survey on security challenges and solutions in the IOTA. *Journal of Network and Computer Applications*, 103383.
23. Damgård, I. B. (1989). A design principle for hash functions. In *Conference on the theory and application of cryptology*. Springer; (pp. 416–427).
24. Dave, E. (2011). How the next evolution of the internet is changing everything. *The Internet of Things*.
25. Dorai, G., Houshmand, S., & Aggarwal, S. (2020). Data extraction and forensic analysis for smartphone paired wearables and IoT devices. In *HICSS*. (pp. 1–10).
26. Du, Y., Wang, Z., & Leung, V. C. M. (2021). Blockchain-enabled edge intelligence for IoT: Background, emerging trends and open issues. *Future Internet*, *13*(2). https://doi.org/10.3390/fi13020048.
27. Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S., & Amin, R. (2021). Blockchain-based internet of things and industrial IoT: A comprehensive survey. *Security and Communication Networks, 2021*, 1–21.
28. Foundation, I. The complete reference for iota, https://wiki.iota.org/. Last accessed 24 Jan 2023.
29. Ge, C., Liu, Z., & Fang, L. (2020). A blockchain based decentralized data security mechanism for the internet of things. *Journal of Parallel and Distributed Computing, 141*, 1–9.
30. Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. (pp. 3–16).
31. Gilbert, H., & Handschuh, H. (2004). Security analysis of sha-256 and sisters. In *Selected areas in cryptography: 10th Annual international workshop, SAC 2003, Ottawa, Canada, August 14–15, 2003. Revised Papers 10*. Springer, (pp. 175–193).
32. Golpîra, H., Khan, S. A. R., & Safaeipour, S. (2021). A review of logistics internet-of-things: Current trends and scope for future research. *Journal of Industrial Information Integration, 22*, 100194.
33. Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Sadoun, B. (2019). Habits: Blockchain-based telesurgery framework for healthcare 4.0. In *2019 International conference on computer, information and telecommunication systems (CITS)*. (pp. 1–5). IEEE.
34. Hajjaji, Y., Boulila, W., Farah, I. R., Romdhani, I., & Hussain, A. (2021). Big data and IoT-based applications in smart environments: A systematic review. *Computer Science Review, 39*, 100318.
35. Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks, 2*, 130–139.
36. Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., & Li, K. (2021). A blockchain-based auditable access control system for private data in service-centric IoT environments. *IEEE Transactions on Industrial Informatics, 18*(5), 3530–3540.
37. Hudson, F., & Clark, C. (2018). Wearables and medical interoperability: The evolving frontier. *Computer, 51*(9), 86–90.
38. Huhn, S., Axt, M., Gunga, H., Maggioni, M. A., Munga, S., Obor, D., Sié, A., Boudo, V., Bunker, A., Sauerborn, R., Bärnighausen, T., & Barteit, S. (2022). The impact of wearable technologies in health research: Scoping review. *JMIR MHealth UHealth, 10*(1), e34384.
39. Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (Healthchain): Evaluation and proof-of-concept study. *Journal of Medical Internet Research, 21*(8), e13592.
40. Infante, R. (2019). *Building Ethereum Dapps: Decentralized applications on the Ethereum blockchain*. Manning Publications.
41. Jiang, D., & Shi, G. (2021). Research on data security and privacy protection of wearable equipment in healthcare. *Journal of Healthcare Engineering*, *2021*.
42. Khan, A. A., Laghari, A. A., Shaikh, A. A., Dootio, M. A., Estrela, V. V., & Lopes, R. T. (2022). A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF). *Neuroscience Informatics, 2*(1), 100030.
43. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)*. (pp. 839–858). IEEE.
44. Kraus, D., Obrist, T., & Hari, O. (2019). *Blockchains, smart contracts, decentralised autonomous organisations and the law*. Edward Elgar Publishing.
45. Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems, 120*, 13–25.
46. Leeming, G., Cunningham, J., & Ainsworth, J. (2019). A ledger of me: Personalizing healthcare using blockchain technology. *Frontiers in Medicine, 6*, 171.
47. Lu, Y., Li, P., & Xu, H. (2022). A food anti-counterfeiting traceability system based on blockchain and internet of things. *Procedia Computer Science, 199*, 629–636.
48. Mercan, S., Cebe, M., Tekiner, E., Akkaya, K., Chang, M., & Uluagac, S. (2020). A cost-efficient IoT forensics framework with blockchain. In *2020 IEEE International conference on blockchain and cryptocurrency (ICBC)*. (pp. 1–5). IEEE.

49. Mills, A. J., Watson, R. T., Pitt, L., & Kietzmann, J. (2016). Wearing safe: Physical and informational security in the age of the wearable device. *Business Horizons, 59*(6), 615–622.
50. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.
51. Namasudra, S., Sharma, P., González Crespo, R., & Shanmuganathan, V. (2022). Blockchain-based medical certificate generation and verification for IoT-based healthcare systems. *IEEE Consumer Electronics Magazine*.
52. Naor, M., & Yung, M. (1989). Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*. (pp. 33–43).
53. Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access, 7*, 85727–85745.
54. Olla, P., & Shimskey, C. (2015). mhealth taxonomy: A literature survey of mobile health applications. *Health and Technology, 4*, 299–308.
55. Özsu, M. T., & Valduriez, P. (1999). *Principles of distributed database systems* (Vol. 2). Berlin: Springer.
56. Özyilmaz, K. R., Doğan, M., & Yurdakul, A. (2018). IDMoB: IoT data marketplace on blockchain. In *2018 Crypto valley conference on blockchain technology (CVCBT)*. (pp. 11–19). IEEE.
57. Pavithran, D., Shaalan, K., Al-Karaki, J. N., & Gawanmeh, A. (2020). Towards building a blockchain framework for IoT. *Cluster Computing, 23*(3), 2089–2103.
58. Pinno, O. J. A., Gregio, A. R. A., & De Bona, L. C. E. (2017). Controlchain: Blockchain as a central enabler for access control authorizations in the IoT. In *GLOBECOM 2017-2017 IEEE global communications conference*. (pp. 1–6). IEEE.
59. Popov, S. (2018). IOTA whitepaper v1.4.3. *New Yorker, 81*(8), 1–28.
60. Pulkkis, G., Karlsson, J., & Westerlund, M. (2018). Blockchain-based security solutions for IoT systems. *Internet of Things A to Z: Technologies and Applications*, pp. 255–274.
61. Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of used cryptography in blockchain. *IEEE Access, 7*, 148550–148575.
62. Raji, R. (1994). Smart networks for control. *IEEE Spectrum, 31*(6), 49–55. https://doi.org/10.1109/6.284793
63. Ramamurthy, B. (2020). *Blockchain in action*. Manning Publications.
64. Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *Journal of Food Quality, 2021*, 1–20.
65. Razdan, S., & Sharma, S. (2022). Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Technical Review, 39*(4), 775–788.
66. rfidjournal.com: That internet of things thing, https://www.rfidjournal.com/that-internet-of-things-thing. Last accessed 24 Jan 2023.
67. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC), 80*, 1–50.
68. Rydningen, E. S., Åsberg, E., Jaccheri, L., & Li, J. (2022). Advantages and opportunities of the iota tangle for health data management: A systematic mapping study. In *2022 IEEE/ACM 5th international workshop on emerging trends in software engineering for blockchain (WETSEB)*. (pp. 9–16). IEEE.
69. Samaniego, M., Jamsrandorj, U., & Deters, R. (2016). Blockchain as a service for IoT. In *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. (pp. 433–436). IEEE.
70. Sengupta, J., Ruj, S., & Das Bit, S. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications, 149*, 102481. https://doi.org/10.1016/j.jnca.2019.102481
71. Shah, S. A., Seker, D. Z., Hameed, S., & Draheim, D. (2019). The rising role of big data analytics and IoT in disaster management: Recent advances, taxonomy and prospects. *IEEE Access, 7*, 54595–54614.
72. Shahab, S., Agarwal, P., Mufti, T., & Obaid, A. J. (2022). Siot (social internet of things): A review. *ICT analysis and applications*, pp. 289–297.
73. Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access, 7*, 147782–147795.
74. Smith, A., Doe, J., Lee, C., Brown, D., & Johnson, E. (2023). Understanding the avalanche effect in cryptographic hash functions. *Journal of Cryptographic Engineering*, pp. 1–14.
75. Somasundaram, R., & Thirugnanam, M. (2021). Review of security challenges in healthcare internet of things. *Wireless Networks, 27*, 5503–5509.
76. Sriman, B., Ganesh Kumar, S., & Shamili, P. (2021). Blockchain technology: Consensus protocol proof of work and proof of stake. In *Intelligent computing and applications*, (pp. 395–406). Springer.
77. Tseng, L., Yao, X., Otoum, S., Aloqaily, M., & Jararweh, Y. (2020). Blockchain-based database in an IoT environment: Challenges, opportunities, and analysis. *Cluster Computing, 23*, 2151–2165.
78. Ullo, S. L., & Sinha, G. R. (2020). Advances in smart environment monitoring systems using IoT and sensors. *Sensors, 20*(11), 3113.
79. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Soler Jubert, I., Mazura, M., Harrison, M., & Eisenhauer, M. (2022). Internet of things strategic research roadmap. In *Internet of things-global technological and societal trends from smart environments and spaces to green ICT*, (pp. 9–52). River Publishers.
80. Voulgaris, S., Fotiou, N., Siris, V. A., Polyzos, G. C., Jaatinen, M., & Oikonomidis, Y. (2019). Blockchain technology for intelligent environments. *Future Internet*, *11*(10). https://doi.org/10.3390/fi11100213.
81. Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for internet of things. *Computer Communications, 136*, 10–29.
82. Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials, 22*(2), 1432–1465.
83. Xu, J., Gu, B., & Tian, G. (2022). Review of agricultural IoT technology. *Artificial Intelligence in Agriculture*.
84. Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet, 11*(4), 94.
85. Zhu, X. N., Peko, G., Sundaram, D., & Piramuthu, S. (2021). Blockchain-based agile supply chain framework with IoT. *Information Systems Frontiers*, pp. 1–16.

Francisco Moya is currently a Ph.D. student in the Computer Science Department at the University of Jaén, Jaén, Spain. He has been involved in research since 2015, focusing on different topics such as multi-criteria decision making, fuzzy logic-based systems, activity recognition and recommender systems. Currently, his Ph.D. research is focused on IoT and blockchain technologies, seeking ways to improve their applicability in various contexts. Additionally, he works as a Software Architect on top tech projects at Inditex.

Francisco J. Quesada received the B.S. and M.S. degrees in Computer Science, a M.S. degree in Education and the Ph.D. degree (specialised in ICT) from the University of Jaén. In 2015, he was a Marie Curie Early-Stage Researcher at the University of Edinburgh, obtaining the Ph.D. degree (specialised in Ontology Matching). He has been an Assistant Lecture since 2020, with the University of Cádiz (from 2020 to 2022) and the University of Jaén (from 2022). He is member of the "Intelligent Systems Based on Fuzzy Decision Analysis" Research Group. His current research interest includes Distributed Ledger Technologies, Group Decision Making, Ontology Matching, IoT, and Emergency Response.

Luis Martínez is currently a Full Professor with the Computer Science Department, University of Jaén, Jaén, Spain. He is also Visiting Professor in University of Technology Sydney, University of Portsmouth (Isambard Kingdom Brunel Fellowship Scheme), and in the Wuhan University of Technology (Chutian Scholar). He has been main researcher in 16 R &D projects, also has published more than 250 papers in journals indexed by the SCI and more than 200 contributions in Inter/national Conferences related to his areas. His current research interests include multi-criteria decision making, fuzzy logic-based systems, computing with words and recommender systems. He was a recipient of the IEEE Transactions on fuzzy systems Outstanding Paper Award 2008 and 2012 (bestowed in 2011 and 2015, respectively). He is a Co-Editor-in-Chief of the International Journal of Computational Intelligence Systems and an Associate Editor of the journals, including the Information Sciences, Knowledge Based Systems, Information Fusion. He is IFSA Fellow 2021, senior member of IEEE and of the European Society for Fuzzy Logic and Technology. Eventually, he has been appointed as Highly Cited Researcher 2017-2022 in Computer sciences.



Fco Javier Estrella received his B.Sc., M.Sc. and Ph.D. degrees in Computer Science, all of them from the University of Jaén in 2008, 2011 and 2015 respectively. His Ph.D. was focused on linguistic preference modeling, decision making, fuzzy logic and consensus reaching processes. After finishing his Ph.D. studies, he focuses on the use of DLTs in different domains such as IoT, big data or digital identity. He was CTO of GeoDB from 2018 to 2021, a startup focused on creating a big data marketplace employing DLT. Since 2022 he is CTO and co-founder of NeoKe, a startup focused on the application of SSI on the connected trip.