Decentralising the Internet of Medical Things with Distributed Ledger Technologies and Off-Chain Storages: A Proof of Concept

Gioele Bigini[1(✉)], Valerio Freschi[1], Alessandro Bogliolo[1,2], and Emanuele Lattanzi[1]

[1] Department of Pure and Applied Sciences, University of Urbino, Piazza della Repubblica 13, 61029 Urbino, Italy
g.bigini@campus.uniurb.it
[2] DIGIT srl, Corso Garibaldi 66-68, 61029 Urbino, Italy

Abstract. The privacy issue limits the Internet of Medical Things. Medical information would enhance new medical studies, formulate new treatments, and deliver new digital health technologies. Solving the sharing issue will have a triple impact: handling sensitive information easily, contributing to international medical advancements, and enabling personalised care. A possible solution could be to decentralise the notion of privacy, distributing it directly to users. Solutions enabling this vision are closely linked to Distributed Ledger Technologies. This technology would allow privacy-compliant solutions in contexts where privacy is the first need through its characteristics of immutability and transparency. This work lays the foundations for a system that can provide adequate security in terms of privacy, allowing the sharing of information between participants. We introduce an Internet of Medical Things application use case called "Balance", networks of trusted peers to manage sensitive data access called "Halo", and eventually leverage Smart Contracts to safeguard third party rights over data. This architecture should enable the theoretical vision of privacy-based healthcare solutions running in a decentralised manner.

Keywords: Decentralised Health Data Management · Internet of Medical Things · Distributed Ledger Technology · Distributed Storage System

1 Introduction

The Internet of Medical Things (IoMT) devices generate a considerable amount of valuable data of inestimable value. However, sharing sensitive information

This research was funded by Regione Marche with DDPF n. 1189 and by the Department of Pure and Applied Sciences, University of Urbino.

I. M. Pires et al. (Eds.): GOODTECHS 2021, LNICST 401, pp. 80–90, 2021.
https://doi.org/10.1007/978-3-030-91421-9_7

between devices is limited by privacy regulations with good intentions but definitely impacting innovation. Solving the sharing problem could significantly impact the health of an individual.

Distributed Ledger Technology (DLT) is a promising technology to solve the sharing issue in IoMT. With the term DLT, we often refer to the technology that allows the transfer of digital assets in a distributed network. In a DLT, every transaction is transparent and visible to all the participants that secure immutability. A specific derivative of DLT is the Blockchain, a well-defined DLT implementation where the ledger consists of a chain of blocks linked together by hashes. The first known implementation is Bitcoin [15]. One of the most significant technology trends during the last ten years is to think of it as general-purpose, i.e. to use it to transfer data or to use it to track digital and real-world items. In this sense, immutable ledgers could enable data ownership, linking a digital asset to an individual. An example of DLT is the IOTA Tangle [19] that is a scalable DLT whose goal is to establish a solution for the IoT by using a Distributed Acyclic Graph (DAG) ledger. A proper feature of IOTA is the ability of being feeless, allowing free transactions. Examples of general-purpose Blockchains are Ethereum and Cardano. Ethereum 2.0 [2] is a Proof of Stake (PoS) protocol that represents the solution for the scalability of the Ethereum blockchain. A similar approach comes from Cardano that is a blockchain platform based on a peer-reviewed PoS protocol called Ouroboros [8].

Several DLTs integrate Smart Contracts that are a set of promises and protocols specified in digital form within which the parties perform on these promises [25]. One of the most interesting facts about Smart Contracts is the possibility to involve them in data sharing. Several general-purpose Blockchain platforms as the most famous Ethereum, Cardano, and IOTA implement Smart Contracts. A platform that is basing his workflow on Smart Contracts is Filecoin [6], a distributed network based on the Blockchain where miners are elected based on the amount of storage in their possession, allowing both the circulation of cryptocurrency in the network and the usage of storages made available by the miners. In fact, Filecoin is a platform designed to grant easy access to decentralised storage, such as the InterPlanetary File System (IPFS).

The biggest concerns that justify the deepening of DLTs for data sharing and decentralisation (potentially Big Data decentralisation) are scalability, since DLTs are not the best for storing extensive data due to their architecture, and compatibility with standards, as the Fast Healthcare Interoperability Resources (FHIR) [1] used to share health data in the healthcare industry. For the scalability issue, it could be convenient to couple DLT with the Distributed File System (DFS), a file system that allows the storage of files and resources in storage devices distributed on the network's nodes. An example of DFS is the previously cited IPFS, a peer to peer distributed file system where peer nodes do not have to trust each other to store and access data on the IPFS network, which makes it similar to the features offered by DLTs (as it supports decentralisation) but with a throughput higher when dealing with large chunks of data, which are stored with the cryptographic hash of their content. Moving to

standards instead, DLTs are promising on boosting their adoption. The FHIR standard defines how healthcare information can be exchanged abstracting from how data is stored. So, it allows healthcare information to be more accessible but, it does not consider the possibility of healthcare systems decentralisation.

While both the DFS and DLT could be private and restricted to a consortium of participants, the choice of using them this way goes against decentralisation. To fix the problem, the usage of cryptography could be essential. The idea is to encrypt to the point that only those who have the credentials can read the files and so, the creator (or the authoritative holders).

In this work, we try to give a possible solution based on DLTs and off-chain storages to decentralise the IoMT and enable a secure data sharing mechanism across the IoMT network. We will show how this solution could work beside an IoMT smartphone application called "Balance", based on the work of E. Lattanzi et al. [11]. The work is structured as follows: Sect. 1, the introduction; Sect. 2, the case study; Sect. 3, the proposed solution; Sect. 4, the discussion and conclusions.

1.1 Related Works

There are many works available on decentralised data management, focusing attention on the sensitivity of health data and, therefore, on attempting to produce a shift to the decentralised paradigm. Most of them use multiple technologies, including decentralised storages such as IPFS, DLTs technologies as Blockchain or DAG, and sometimes cryptography. The key idea for each work is to connect patients and any health organisations and enable users to own data created. One of the most significant research in the field [17] uses the Ethereum network to save data through links saved on the Blockchain assisted by Smart Contracts. Moreover, the paper introduces the usage of mobile devices, i.e. the smartphones. Another interesting approach [13], in addition to IPFS and Smart Contracts, attempts to introduce a reputation system to encrypt and share data. An incremental solution to the latter [5] introduces an economic incentive for those who disseminate their health data since these effectively contribute to a piece of greater knowledge for personalised medicine. Similar idea on the usage of IPFS and Smart Contracts also belongs to other researchers [14,24], with some exception [10,23] which respectively uses IPFS, Blockchain and cloud technologies. On the other hand, others have focused mainly on monitoring practices, such as teleconsultation [9] or specific tracking-related problems such as organ transplantation [21] or more general health data [16]. Other works than look to the effective compliance of these systems with the healthcare sector [18], or the possibility of providing an identity to the participants anticipating a Health Digital Identity System. Finally, more complex works [7,26] use multiple blockchains intending to give different roles to the different players involved and separate systems for data management.

Other few solutions are based on the IOTA Tangle, addressing different issues. The first identified issue focus on the fact that patients and healthcare organisations must communicate and therefore be interoperable [22]. The research

tries to understand the actual current standards used in health institutions to provide an approach that can be integrated with these standards already used in hospitals, including the Fast Healthcare Interoperability Resources (FHIR). In the paper, they try to use the Tangle with the already existing standards and, therefore, save the data produced by patients in the EHR systems of health institutions. The attempt is undoubtedly interesting and demonstrates the possibility of using these standards with DLT technologies. Other researchers instead focuses on studying the scalability of the blockchain in healthcare institutions [4]. That is, they try to understand if the available DLTs technologies are suitable for use in the presence of large volumes of transactions. Cardano in the paper is the best performer of technologies with the least need to use sidechains in order to speed up transactions. Similar works for data sharing have been investigated [12]. The idea is based on the Tangle and data owners interact with it through mobile devices. The Tangle is used for saving data but we think that it is also not recommended for privacy reasons, since the ledger is basically immutable. Authors of [3] focused on COVID-19 pandemic monitoring operations. The paper attempts to focus on emergency and response issues. The idea is to use the Tangle as a data layer used by local authorities and the US government locally for emergency management. It is unclear how the user can be the data owner since his interaction does not occur with the ledger but with institution-owned databases that potentially replicate data.

1.2 Contribution of This Paper

In the future, the possibility for individuals to manage their sensitive information could lead to the creation of billions of everlasting clinical histories useful to enhance new medical studies, formulate new treatments, and deliver new digital health technologies. Decentralisation could be inevitable, eclipsing central authorities as store of sensitive information, being replaced by individuals responsibility. This work propose an idea on how to decentralise the IoMT by presenting a case study with the aim of enabling data ownership, and sharing. Participants avoid revealing data locations on distributed storages and manage their data through decentralised private networks called Halo. In our solution, we propose the use of off-chain storages, DLTs, Smart Contracts, mobile devices, and the introduction of the Halo: networks of participants who secure and manage data against remote stakeholders. This will guarantee no direct access to data locations and that remote users would always be tracked and forced to accept sharing conditions.

2 The Case Study

Balance is a IoMT smartphone application that records the human postural stability indices of an individual through the sensors integrated within the smartphone. It aims to produce a stabilometric analysis by referencing the biomechanical model of the single inverse pendulum and the available traditional healthcare technology in the field [11]. The stabilometric analysis allows evaluating the

patient's stability in the upright position by studying the dynamics of the center of gravity projection on a plane parallel to the ground. The smartphone application carry out the analysis with this scope, since the human sensory system can be considered at rest (except for the plantar skin receptors), and so, the body instability is reconducted to endogenous factors. During a static test, the patient is stationary and standing on a measurement surface with his eyes open or closed, without the presence of any external perturbation. The body moves due to the combination of internal correction forces, drawing the deformation they produce on the underlying plane. The point of force application is called the center of pressure (COP) since it is the center of the distribution of pressure on the surface of the foot.

2.1 Architecture

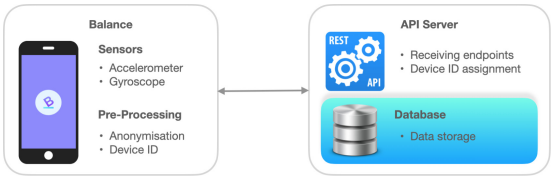

Fig. 1. Balance architecture

Balance architecture consists of a mobile application and a backend that resides in a centralised location (Fig. 1). The smartphone application performs all the pre-processing onboard the smartphone in order to comply with privacy regulations. The data is sent to the backend in a completely anonymous way. A unique ID generated by the backend and not associated with the user or his device is sent to the user to always refer to his data correctly.

2.2 Measurement Protocol

In traditional systems, the subject is placed at the center of a force platform for postural acquisition to perform the required test. In the case study, the Romberg test that is a test in which the patient performs the analysis with both eyes open or closed, allowing to understand the influence of the visual system on posture.

Through Balance, the repeatable test is performed through the smartphone in a few seconds. The test can be carried out with open or closed eyes by choosing the appropriate mode on the home screen. While performing a test, the user keeps a straight posture and holds the smartphone with two hands in a vertical position at the navel level, guided to maintain the correct position. The actual sensor measurement takes about 30 s. For the analysis to be meaningful, the test must be repeated periodically. In this way, it is possible to compare the past indices with the most recent ones and monitor the evolution of postural stability.

2.3 Data Collected

The static analysis generates two main insights: the statokinesigram (SKG), or sway-path, represents the displacement of the COP in the X,Y plane and allows for the extraction of global parameters and structural parameters; the former relates to the sway-pattern while the latter focus on trajectories applicable to extracting data from them. The Stabilogram, shows the change in COP over time expressed as a vector in two dimensions: Antero-Posterior (AP) and Medio-Lateral (ML).

The user is also asked for some personal information: age, gender, weight, any postural problems, the presence of postural problems in the family, the use of medicines that can interfere with posture, any other trauma, visual defects, and hearing defects. Potentially, it will be possible to extend and use them for several reasons that go from performing medical studies to personalised medicine.

3 The Proposed Solution

3.1 DLTs Comparison

It is worthwhile to evaluate several DLTs candidates for a decentralised data management solution. In this section we analyse Ethereum 2.0, Cardano, Filecoin and, IOTA 2.0 which results are shown in Table 1.

Based on the comparison, Cardano is going to provide the most appreciable result in terms of long-term objectives, promising the best results both from the Governance and the tps. A good compromise represents IOTA 2.0, which would allow greater freedom regarding the reduction of the cost of transactions. A little in the shadows is Ethereum 2.0, which does not seem to promise a high number of tps as the other implementations, even if it is good to highlight how it represents a consolidated Blockchain and it has the best development ecosystem worldwide. Finally, Filecoin represents an ad-hoc solution to be adopted for specific needs.

Table 1. DLTs Comparison *Highly Speculative

Category	Ethereum 2.0	Cardano	Filecoin	IOTA 2.0
DLT	Blockchain	Blockchain	Blockchain	DAG
General Purpose	Yes	Yes	No	Yes
Consensus	PoW/PoS	PoS	PoW	No/FPC
Smart Contracts	Yes	Yes	Yes	Yes
Dynamic Governance	No	Yes	No	No
Feeless	No	No	No	Yes
Transactions Per Second	15/*100k	250/*1m	Not Known	200/*300k

Ethereum 2.0. The biggest problems Ethereum 1.0 is suffering are higher transaction fees and low tps. The upgrade to the second version is to overcome both the problems, by replacing the Proof Of Work protocol with a PoS protocol. On the side of Governance, Ethereum is not so dynamic. Users, miners and developers can submit proposals but, on Github. The biggest obstacle to this is finding support for that proposal that needs to reach the Core developers through several channels like social media, conferences, articles. Once the proposal attracts interest could be taken into consideration. In the future, It is expected that Ethereum 2.0 could bring more than 100 thousand tps increasing the actual stage of about 15 tps.

Cardano. Thanks to Ouroboros, Cardano is one of the most scalable blockchains in the crypto-space with 250 tps on average, basing its success on its community of stake pools, actively contributing to the security of the network. Moreover, It has a dynamic governance system based on democratic voting on upgrade proposals that ensures the platform and its community can continuously fund and decide upon platform and ecosystem improvements. In the future, the system will implement a second layer solution under research called Hydra that is going to bring the tps to more than 1 million, a great achievement for the overall crypto-space.

IOTA 2.0. Unlike the first version of IOTA, where a centralised entity called coordinator was validating the transactions milestones (a checkpoint in the Tangle that was validating all the backward transactions), IOTA 2.0 will operate decentralised by introducing several features summed up in the Coordicide paper [20], designed to be modular and to ensure long-term success. Note that the second version is going to implement a Fast Probabilistic Consensus (FPC). IOTA governance is centralised but the development team is open to conversations. Several components have been developed between IOTA and community members. By the way, they do not have a voting system in this sense, but at least it is all transparent. Industry players help guide the development of the system. In the future, the Tangle is expected to bring more than 300 thousands tps.

Filecoin. Filecoin is a Blockchain with the specific aim to give permanence to data in a decentralised environment. Even if It is actually not seen as general-purpose, in addition to allow transactions, the Filecoin ledger implements Smart Contracts, and it implements a proprietary Virtual Machine (Filecoin VM) that offers control mechanisms that regulate the operation and acquisition of decentralised storage requested by the users. We could think of Filecoin as the first attempt to exploit Blockchain technology to achieve persistence of stored data on decentralised storages through paid agreements exactly as happening with the cloud technology. The system rewards participants as a mean of incentive for all who are willing to provide data storage.

3.2 Architectural View

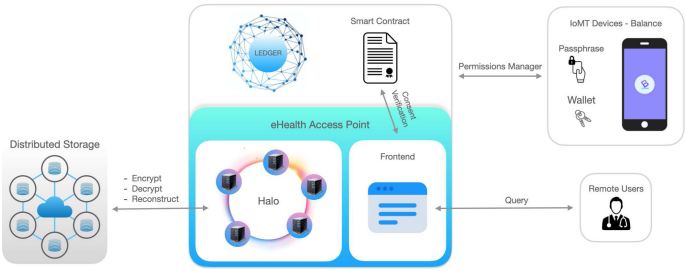

Fig. 2. System architecture

The IoMT comprises mobile devices, i.e. smartphones, devices, wearables. The need for these devices is the ability to perform operations that involve sensitive information. In the following sections, we try to give a view of the components and the architecture to achieve this result.

Components. The components of the architecture must reflect all the needs foreseen in the IoMT. A reference to the architecture is in Fig. 2 and includes:

- The IoMT Device is the location where the user's data are generated and the private keys, used for signing data, are stored. Safety issues relating to the device used are neglected. Through the Wallet, it is possible to access the Ledger and manage digital assets.
- The Ledger gives the user a potential anonymised criterion of being uniquely identified in the network.
- Smart Contracts are used to grant access to remote users using Non-Fungible Tokens (NFTs).
- Remote users represent all those interested parties in accessing sensitive information. They can be professionals, general users and healthcare organisations. The interaction happens through the web interface.
- The proposed Halo is a private network, similar to a oracle network, of explicitly trusted nodes which is involved in encrypting, decrypting, and reconstructing user's off-chain data, guaranteeing availability. Their role is of redundancy and data security.
- The Distributed Storage is where the data of the user are saved. Decentralised technologies, such as IPFS, are public storages, transparent and publicly accessible. For this reason, the data on the storage are sharded and anonymised, and the private network needs to reconstruct the data properly.

Workflow. Storing data from the IoMT devices should follow the steps shown in Fig. 3:

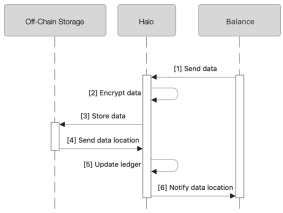

Fig. 3. Data store diagram

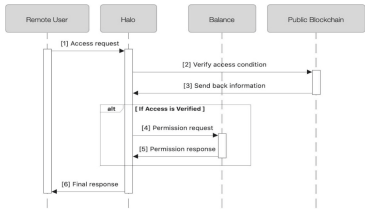

Fig. 4. Data sharing diagram

1. The system is composed of a wallet containing the cryptographic keys for signing new data. Every time the user generates new data, this is sent to the Halo.
2. Once data are successfully stored, the links to the decentralised storage could be sent to the DLT and saved as transactions or kept private into the smartphone, creating a recovery-proof mechanism.
3. The Halo eventually ensure data pinning to the store files on decentralised storage and privacy-compliant operations before storing.

Sharing information with remote users should follow the process in Fig. 4:

1. A remote user asks for health data by accessing the frontend and accepting conditions.
2. The Halo verifies the access on the public blockchain, ideally with the help of Smart Contracts, and then forwards the request to the data owner device, who is required to give consent.
3. If consent is given, the network processes the data and sends the final response to the user; otherwise, it will just notify the rejection.

4 Discussion and Conclusions

By using the proposed architecture, the health data are created and maintained by the owners. All remote users are subject to predefined rules, and Smart Contract constitutes a transparent way of managing permissions. Cryptography constitutes an essential tool and it will need advancements in the future. In fact, it is not a sufficient deterrent for keeping data secure with the advent of quantum computing, even if coupled with sharding and masking techniques constitutes a solution. It should be noted that this approach causes a decrease in performance by forcing rebuilding before the use. The usage of a two-layer solutions guarantees both transparency and logging, while the usage of Distributed Storages could allow for data relocation since data stored are persistent but not permanent.

In this work, we proposed a solution to decentralise the IoMT, enabling data sharing. Our solution is blockchain agnostic and demonstrates the role of DLT technology as an enabler for sharing sensitive data. The overall architecture could constitute a personal sensitive data portal with which healthcare systems can be

interfaced directly to individuals. Smart Contracts can be essential in establishing agreements between the owner and remote users, highlighting the need for a Decentralised Digital Identity. As future work, we plan to develop the implementation of this solution by using DLTs technologies and IoMT applications to demonstrate the potentiality of the system in solving the sharing problem scenario without relying on any intermediary.

References

1. Bender, D., Sartipi, K.: HL7 FHIR: an agile and restful approach to healthcare information exchange. In: Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems, pp. 326–331 (2013). https://doi.org/10.1109/CBMS.2013.6627810
2. Buterin, V., Griffith, V.: Casper the friendly finality gadget. arXiv preprint arXiv:1710.09437 (2017)
3. Cisneros, B., Ye, J., Park, C.H., Kim, Y.: 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 (2021). https://doi.org/10.1109/CCWC51732.2021.9376093
4. Donawa, A., Orukari, I., Baker, C.E.: Scaling blockchains to support electronic health records for hospital systems. In: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0550–0556. IEEE (2019). https://doi.org/10.1109/UEMCON47517.2019.8993101
5. Fernández-Caramés, T.M., Froiz-Míguez, I., Blanco-Novoa, O., Fraga-Lamas, P.: Enabling the internet of mobile crowdsourcing health things: a mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. Sensors **19**(15), 3319 (2019). https://doi.org/10.3390/s19153319
6. Filecoin: Filecoin - a decentralized storage network designed to store humanity's most important information (2017). https://filecoin.io
7. Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J.: BlocHIE: a blockchain-based platform for healthcare information exchange. In: 2018 IEEE International Conference on Smart Computing (Smartcomp), pp. 49–56. IEEE (2018). https://doi.org/10.1109/SMARTCOMP.2018.00073
8. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: a provably secure proof-of-stake blockchain protocol. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 357–388. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_12
9. Kordestani, H., Barkaoui, K., Zahran, W.: HapiChain: a blockchain-based framework for patient-centric telemedicine. In: 2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH), pp. 1–6. IEEE (2020). https://doi.org/10.1109/SeGAH49190.2020.9201726
10. Kumar, R., Marchang, N., Tripathi, R.: Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In: 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), pp. 1–5. IEEE (2020). https://doi.org/10.1109/COMSNETS48256.2020.9027313
11. Lattanzi, E., Freschi, V., Delpriori, S., Klopfenstein, L.C., Bogliolo, A.: Standing balance assessment by measurement of body center of gravity using smartphones. IEEE Access **8**, 96438–96448 (2020). https://doi.org/10.1109/ACCESS.2020.2996251

12. Lücking, M., Manke, R., Schinle, M., Kohout, L., Nickel, S., Stork, W.: Decentralized patient-centric data management for sharing IoT data streams. In: 2020 International Conference on Omni-layer Intelligent Systems (COINS), pp. 1–6. IEEE (2020). https://doi.org/10.1109/COINS49042.2020.9191653
13. Madine, M.M., et al.: Blockchain for giving patients control over their medical records. IEEE Access **8**, 193102–193115 (2020). https://doi.org/10.1109/ACCESS.2020.3032553
14. Marangappanavar, R.K., Kiran, M.: Inter-planetary file system enabled blockchain solution for securing healthcare records. In: 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), pp. 171–178. IEEE (2020). https://doi.org/10.1109/ISEA-ISAP49340.2020.235016
15. Nakamoto, S.: Re: Bitcoin p2p e-cash paper. The Cryptography Mailing List (2008)
16. Nascimento Jr, J.R., Nunes, J.B., Falcão, E.L., Sampaio, L., Brito, A.: On the tracking of sensitive data and confidential executions. In: Proceedings of the 14th ACM International Conference on Distributed and Event-based Systems, pp. 51–60 (2020). https://doi.org/10.1145/3401025.3404097
17. Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A.: Blockchain for secure EHRS sharing of mobile cloud based e-health systems. IEEE Access **7**, 66792–66806 (2019). https://doi.org/10.1109/ACCESS.2019.2917555
18. Omar, I.A., Jayaraman, R., Salah, K., Simsekler, M.C.E., Yaqoob, I., Ellahham, S.: Ensuring protocol compliance and data transparency in clinical trials using blockchain smart contracts. BMC Med. Res. Methodol. **20**(1), 1–17 (2020). https://doi.org/10.1186/s12874-020-01109-5
19. Popov, S.: The tangle. White Paper **1**, 3 (2018)
20. Popov, S., et al.: The coordicide, pp. 1–30 (2020). Accessed Jan
21. Ranjan, P., Srivastava, S., Gupta, V., Tapaswi, S., Kumar, N.: Decentralised and distributed system for organ/tissue donation and transplantation. In: 2019 IEEE Conference on Information and Communication Technology, pp. 1–6. IEEE (2019). https://doi.org/10.1109/CICT48419.2019.9066225
22. Saweros, E., Song, Y.T.: Connecting personal health records together with EHR using tangle. In: 2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp. 547–554. IEEE (2019). https://doi.org/10.1109/SNPD.2019.8935646
23. Seliem, M., Elgazzar, K.: BioMT: blockchain for the internet of medical things. In: 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), pp. 1–4. IEEE (2019). https://doi.org/10.1109/BlackSeaCom.2019.8812784
24. Sultana, M., Hossain, A., Laila, F., Taher, K.A., Islam, M.N.: Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med. Inform. Decis. Mak. **20**(1), 1–10 (2020). https://doi.org/10.1186/s12911-020-01275-y
25. Szabo, N.: Formalizing and securing relationships on public networks. First Monday (1997). https://doi.org/10.5210/fm.v2i9.548
26. Xu, J., et al.: Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things J. **6**(5), 8770–8781 (2019). https://doi.org/10.1109/JIOT.2019.2923525