KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 7 (2021) 308–315

www.elsevier.com/locate/icte

BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten

Eugenio Balistri[a], Francesco Casellato[a], Carlo Giannelli[b,*], Cesare Stefanelli[a]

[a] *Dept. of Engineering, University of Ferrara, Italy*
[b] *Dept. of Math and Computer Science, University of Ferrara, Italy*

Received 28 February 2021; received in revised form 21 June 2021; accepted 2 August 2021
Available online 20 August 2021

Abstract

To identify health risks in working environments, it is crucial for companies to share personal health data demonstrating to clients and suppliers their employees are healthy, while being compliant with data protection legislation. Based on these considerations, our Blockchain-based BlockHealth solution allows personal health data sharing with tamper proofing and data protection. Traditionally, the Blockchain guarantees data immutability but not confidentiality. On the contrary, BlockHealth stores in the Blockchain only hash values of data. Health data is stored in private databases managed by companies, thus also allowing to delete data in compliance with the right to be forgotten.

Keywords: Blockchain; Health monitoring; Data sharing; Data protection; Right to be forgotten

1. Introduction

The SARS-Cov-2 virus epidemic and the COVID-19 infection have demonstrated how timely identification of outbreaks is essential to limit their spread. It is in the interest of companies and the community to transform companies into checkpoints for the active surveillance of workers to protect individual and community health. To this purpose, many companies are organizing themselves to autonomously perform virus detection tests (with serological and/or molecular periodic tests) on their employees. Within this framework, it is also crucial to ensure that these tests are performed in full compliance with the local legislation related to personal data protection (and especially of health data) of every involved individual. For instance, the European General Data Protection Regulation (GDPR) [1] specifically defines data concerning health as a special category of data "which reveal information relating to the past, current or future physical or mental health status of the data subject". Moreover, it also states that to ensure that individuals can have trust and confidence on systems and people in charge of managing their health data, it is required to enforce robust data protection safeguards.

To achieve these goals, we state that there is the need of innovative data management approaches that allow to share health data among companies, since the sharing of such data is of paramount importance to enforce quick and effective countermeasures to health threats. Moreover, health data must be shared in a secure and immutable manner, also in case there is no third-party acting as trust actor. The objective is to foster a participatory data management process stemming from data producers, rather than only being pushed from government entities (while not denying their participation, if possible). At the same time, we fully recognize the right of citizens to keep control on their personal health data, in particular of their right to completely delete every data related to them, in case they desire so.

Based on these considerations, we designed and developed the BlockHealth solution for active surveillance and sharing of health data with tamper proofing and data protection guarantees. The main contribution of our original solution is to collect and share health data while achieving the twofold objective, on the one hand, of ensuring data immutability, and on the other hand, of guaranteeing not only personal data protection but also the right to be forgotten of each individual. By achieving such objectives, we are able to address issues related

* Corresponding author.
E-mail addresses: eugenio.balistri@unife.it (E. Balistri), francesco.casellato@unife.it (F. Casellato), carlo.giannelli@unife.it (C. Giannelli), cesare.stefanelli@unife.it (C. Stefanelli).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.08.006

to the sharing of health test data among companies working in the same territory and/or in the same production chain. For instance, such a solution can be adopted for the proper management of data revealing the presence of the COVID-19 infection, as well as of data suggesting a different health issue may exist.

In addition, with the BlockHealth solution we contribute to improve the state-of-the-art also from a practical point of view by designing, implementing, and testing a Blockchain-based technological infrastructure allowing the development of a distributed clinical test register, shared among different companies. Such a novel contribution allows different companies participating in the same Blockchain to access their data also certifying the immutability of recorded data, even without the participation of any public authority. In comparison with traditional solutions based on a centralized data repository, a key innovative aspect of our solution is it ensures the most efficient trade-off between health protection, personal data protection, scientific and technological progress, and production efficiency, in line with state-of-the-art legislation trends. Let us stress that a solution valid from a technological point of view but not complying with current regulations cannot be applied by companies. Also note that the proposed solution is agnostic in relation to the specific immunological test that will be adopted and can be applied regardless of the specific health data that will be actually shared among companies.

2. The BlockHealth solution

2.1. Blockchain primary aspects

To better present the proposed solution, we briefly introduce most relevant characteristics of the Blockchain technology. In fact, Blockchain represents an articulated ecosystem encompassing several well-known technologies, ranging from symmetric and asymmetric cryptography to peer-to-peer distributed management based on consensus algorithms. Readers interested in an in-depth and complete introduction to Blockchain can refer to [2–4].

First of all, it is worth noting that a Blockchain can store information of any type, thus without any constraint in terms of syntax and semantic. In particular, a Distributed Ledger Technology (DLT) is a sequence of time-ordered transactions agreed among peers by adopting a distributed consensus algorithm. A Blockchain specializes the DLT by grouping transactions in immutable and linked blocks; each block is strictly correlated to the block before and the block after via secure hashes and cannot be modified once added to the Blockchain. The first block, namely the genesis block, is the only one without a previous block. New blocks can only be added after the current last block, and only if (part of) nodes hosting a copy of the ledger agree based on a given consensus algorithm. Once a block is added at the head of the ledger it cannot be modified, thus a Blockchain is an inherently incremental DLT whose past data are immutable.

In a Blockchain, smart contracts further specialize a DLT by restricting how transactions can be generated and which kind of information transactions can contain. For instance, a smart contract can limit nodes to create a new transaction only if some conditions apply, e.g., previous transactions of the same ledger have some information and external entities provide some resources. More technically, the creation of a new transaction based on a smart contract imposes that some code is executed on some data; the achieved output represents the body of the new transaction.

Despite the Blockchain is exploited either to create a generic DLT or to enforce a smart contract, to create a new transaction nodes managing copies of the same ledger must cooperate and agree one each other. To this purpose, when a node requires to add some data to the ledger, it creates a new transaction and sends it to other nodes (usually interacting in a peer-to-peer fashion). Involved nodes apply a given consensus algorithm to either accept or refuse the new transaction: in the former case, the transaction is inserted into a block and eventually added to every copy of the ledger, in the latter case the transaction is discarded.

Another important distinction among Blockchain solutions is permissionless vs. permissioned. In the former case, there is no restriction on nodes joining the Blockchain. For instance, this is the case of Bitcoin, a cryptocurrency allowing anyone to create transactions to move crytpovalue from a wallet to another. In the latter case, only authenticated nodes can participate in the network. The number of involved nodes is typically limited while the level of trust is higher.

2.2. Blockchain for privacy preserving data sharing

By appropriately adopting the Blockchain as data sharing platform, our novel BlockHealth solution guarantees that the processing of personal health data (e.g., COVID-19 test outcomes) provided by companies complies with following requirements:

- access to information only by legitimate subjects (e.g., health or judicial authorities). To this purpose, it should be possible to access shared data only if authenticated and authorized;
- data immutability. Once data have been shared, it should not be possible to modify any data, even the timestamp related to their creation and/or sharing;
- privacy and right to be forgotten of monitored people. While data cannot be modified, it should be possible to completely delete them, thus ensuring that starting from the delete procedure nobody can access them anymore;
- data minimization and proportionality of the treatment to the pursued aim. Only people in charge of managing the full content of the data should be able to access them without any restriction. On the contrary, actors needing to access only a subset of information should selectively access only strictly required data.

The proposed BlockHealth solution represents a significant progress compared to the usual adoption of Blockchain technology. In fact, Blockchain solutions traditionally have the advantage of guaranteeing the immutability of data but do

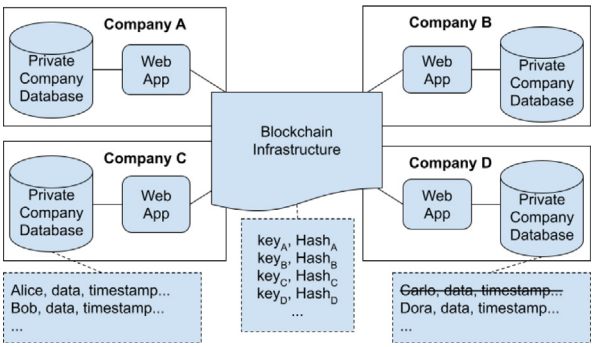


Fig. 1. High-level representation of the BlockHealth architecture.

not ensure its confidentiality, to the extent that they allow every participant of the Blockchain infrastructure to have full access and visibility of data within blocks. Let us stress that the originality and the added value of the proposed approach are that it provides a solution that is not only tamper-proof (once data has been inserted it is impossible to modify it, or any modification can be easily identified) but also privacy-preserving (data can only be accessed by legitimate staff and, if required, it can be also deleted).

To this purpose, BlockHealth does not insert in the Blockchain the health data, e.g., outcomes of serological COVID-19 tests, but rather only their secure hash. Actual health data is exclusively stored in a private database owned by (and under the control of) each different company. The truthfulness of provided data will be guaranteed by the fact that the secure hash of health data will be stored in the Blockchain, shared between different companies in an immutable way and associated with a timestamp. In this way, the Blockchain will continue to permanently maintain only secure hashes of data and therefore it will be impossible, for subjects not legitimated to do this, to reconstruct the related health data.

To better present the proposed solution, Fig. 1 outlines primary BlockHealth modules:

- Private Company Database (PCD). Each company has its own private database (managed independently) where it maintains personal health data of its own employees. For instance, for each serological test, it stores not only the identity of the tested employee, the timestamp, and the outcome, but additional information such as the place where the test has been done and the doctor in charge of signing the outcome of the test;
- Blockchain Infrastructure (BI). Peer-to-peer Blockchain network composed of nodes hosted by the companies adopting the solution. Each transaction contains the hash value of personal health data related to a person and a key identifying that data, e.g., the concatenation of company name, employee full name, and timestamp. Once added to the Blockchain, such information cannot be modified and thus it is possible to verify if the data stored in the PCD have been modified after their insertion;
- Web App (WA). Software component that allows users (subject to authentication and authorization) (i) to add/view/delete health data within the PCD by checking their integrity based on the corresponding secure hash and (ii) to create a Blockchain transaction containing the secure hash of that information (or a subset of such information).

As Fig. 1 shows, each PCB contains the full set of test information, but only of employees of the related company. On the contrary, BI contains only the hash and key values, but of every company. Such values stored in Blockchain transactions are immutable and thus it is possible to verify if health data have been modified after it has been added to BlockHealth. However, information can be deleted from each PCB, thus ensuring to employees the right to be forgotten. In this case, the hash value will be still available on BlockHealth, but actual data will not be stored on the related PCB anymore, making impossible to reconstruct original test outcomes (e.g., see Carlo's data in Fig. 1).

In addition, it is worth noting that health data of a single person can be grouped in several manner, depending on the visibility that it is desired to provide (in compliance with the requirement of data minimization). For instance, an actor could see only minimal information, i.e., identity, COVID-19 test outcome, and date, while another actor could also see other personal and health data, e.g., contact information and blood group. For each subset of data it is required to give selective visibility, BlockHealth generates a different hash, thus allowing to verify the truthfulness of data while still ensuring their differentiated visibility.

3. Architecture overview and performance analysis

3.1. Technology background

To better present our proof-of-concept prototype, this section outlines primary characteristics of adopted technologies. First of all, note that PCB and WA modules together represent a typical Web environment, composed of a database and a Web application. For the former we adopted the open-source PostgreSQL database, but in case the amount and heterogeneity of data considerably increase it would be more suitable to adopt a NoSQL document database such as MongoDB. For the latter we have adopted Ruby on Rails (RoR) since it allows to quickly develop and deploy well-structured and secure Web applications, but other frameworks could be used as well.

Additional considerations must be done for the BI, since as already anticipated in Section 2.1, there are several possible Blockchain solutions, greatly differing in terms of interacting components, supported features, and imposed overhead. Among widely adopted Blockchain solutions, Bitcoin and Ethereum represent notable permissionless ones. Considering that the target environment is composed of a set of well-known companies, we deem more appropriate to adopt permissioned solution. In this manner we can ensure that only authenticated and authorized actors can inject transactions in the BI, with the notable effect of avoiding that fake information can be stored in BlockHealth.

Delving into finer details, we have adopted Hyperledger Fabric [5] as Blockchain platform to develop our BI. Its primary components are:

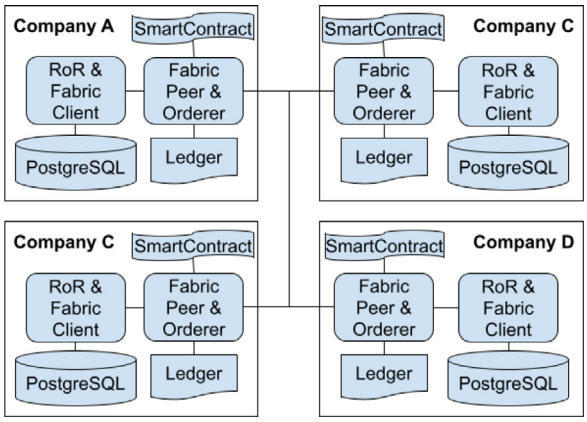


Fig. 2. BlockHealth architecture with technology details.

- *clients*, requiring the creation of a new transaction based on a specific endorsement policy, detailing how to select nodes involved in a transaction creation procedure. To this purpose, clients (i) contact a subset of endorser peers as specified by the endorsement policy, e.g., at least one for each organization involved in the transaction, (ii) wait for a given amount of transaction endorsements, again as specified by the endorsement policy, e.g., by adopting a vote-based consensus algorithm requiring majority/unanimous vote, and (iii) send the new transaction to orderers;
- *peers*, nodes maintaining a local copy of the ledger by committing transactions and updating the ledger whenever they receive a new block. Peers can also execute smart contracts and validate transactions provided by clients;
- *endorsers*, specific peers that can execute smart contracts whenever they receive a transaction proposal. During the endorsement of a new transaction, endorsers securely sign so-called endorsement messages (also containing transaction output, transaction id, endorser id, and endorser signature) and send it to the client requiring the new transaction;
- *orderers*, nodes collecting requests of new transactions creations, grouping multiple transactions in a block, e.g., sorting concurrent transaction requests coming from different clients, and issuing commands to peers to add new blocks on top of the ledger. Note that orderers are unaware of transaction semantics and exploit cryptographic signatures of endorsers to create new blocks.

3.2. Implementation details and performance analysis

We have developed and experimentally verified a working proof-of-concept with the primary goal of not only demonstrating the feasibility of the proposed approach, but also its suitability in terms of performance to add, access, and delete health data. The source code of the BlockHealth working prototype is available through a public repository,[1] useful for testing and for getting feedbacks by companies and other researchers.

Fig. 2 presents the BlockHealth architecture by outlining adopted technologies for each module. The WA module is composed of both the RoR Web application and the Hyperledger Fabric client. The former directly interacts with the PostgreSQL-based PCD module, the latter acts as entry-point of the BI module and supports basic features such as adding new transactions to the Blockchain and retrieving previously stored transactions. The BI module is composed of the Fabric Peer and the Orderer. The former acts both as committer (to locally store a copy of the distributed ledger) and as endorser (to enforce the smart contract), the latter receives endorsed transactions and adds them to new blocks.

Fig. 3 presents a detailed description of the actions required to add new health data in BlockHealth (view and delete data sequence diagrams not presented for the sake of briefness). After the user has been authenticated and authorized by the Web Application, she can send health data to the Web application. Then, health data are managed by the Fabric client, in charge of creating a new transaction request (containing provided health data), sending it to endorsers, and waiting for signed endorsements. Note that endorsers apply the smart contract in charge of generating hash values starting from original health data and in the transaction are stored hash values instead of the original health data. In case the Fabric client receives a proper amount of signed endorsements (depending on the adopted endorsement policy), it forwards the new transaction request together with signed endorsements to the Ordering service, waiting for other transaction requests and generating a new block whenever it receives a sufficient amount of requests. Once the Ordering service generates a new block, it sends the block to endorsers and other remote peers. In particular, the original Fabric client receives a notification that the requested new transaction has been correctly added to a block. Finally, the Web application is notified about the successful creation of the block and can add health data to the private database, also notifying the accomplishment of the procedure to the user.

We have experimentally verified the implemented prototype in a testbed composed of three nodes with relatively limited resources (1 vCPU, 1 GB RAM and 10 GB of disk space with Ubuntu Cloud bionic 18.04.5 LTS), running on top of OpenStack Train, connected via an OpenStack virtual network. Every node represents an organization and on every node we deployed Hyperledger Fabric 2.3.1, with one endorser and one orderer, and the endorsement policy is of type All (every endorser must approve the transaction).

The *addPersonalData* smart contract has been developed in Golang with Fabric Shim, providing low-level API and supporting communication with Hyperledger Fabric peers (see Listing 1 for its primary aspects). First of all, the smart contract verifies the number of parameters passed as argument. It is possible to pass various parameters based on the number of hash values to be created. The key is composed of three values: company, employee full name, and timestamp. In this manner, it is possible to retrieve the record exploiting information related to the person but not providing any health data. For

[1] https://github.com/DSG-UniFE/BlockHealth.

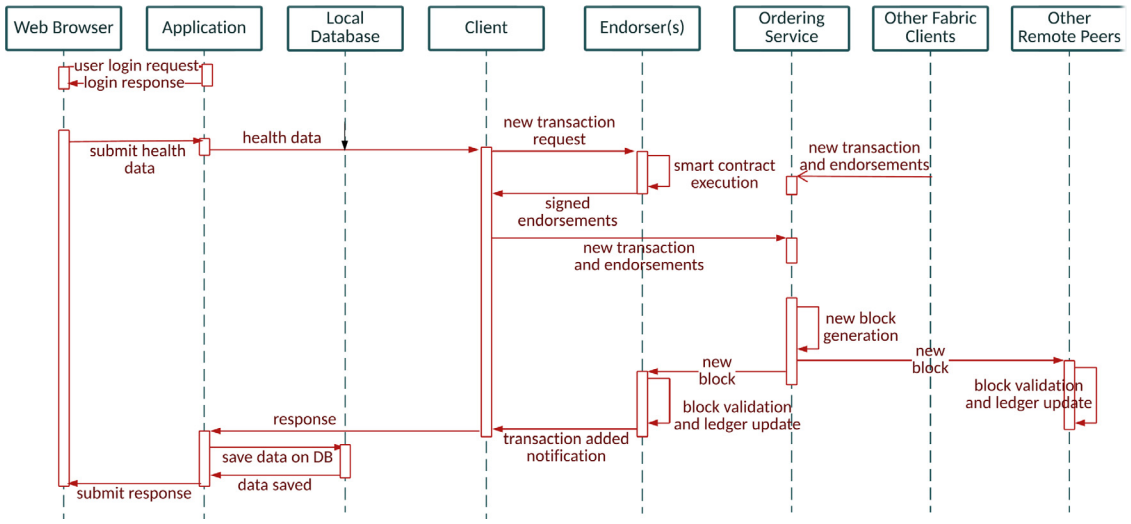


Fig. 3. Insert data sequence diagram.

each transaction, the smart contract creates n_hash subsets of information and then computes their hash values. After that, it iterates the process for each parameter contained in the array named "more". Once done, if it is not already present, it saves the status of the transaction in the Blockchain and finally it notifies the client.

Listing 1: Smart contract to add personal health data.

```
func (s *DataContract) addPersonalData (
 APIstub shim.ChaincodeStubInterface,
 args []string)
 sc.Response {

 if (len(args) < 7 || len(args) >15 ){...}
 // key
 company := args[0]
 fullname := args[1]
 timestamp := args[2]
 // hash array
 var hash_slice [][16]byte
 // other infos
 test_type := args[3]
 result := args[4]
 more := args[5:len(args)-1]
 n_hash,_ := strconv.Atoi(args[len(args)-1])

 // first subset; key + test type
 sub_info := []string{company,
 fullname, timestamp, test_type}
 sub_info_data,_ := json.Marshal(sub_info)
 hash_slice = append(
  hash_slice, md5.Sum(sub_info_data))

 // second subset; key+ type + result
 sub_info = append(sub_info, result)
 sub_info_data,_ = json.Marshal(sub_info)
 hash_slice = append(
  hash_slice, md5.Sum(sub_info_data))

 // other subset
 for i := 0; i < n_hash; i++ {
  sub_info = append(sub_info, more[i])
  sub_info_data,_ = json.Marshal(sub_info)
  hash_slice = append(
   hash_slice, md5.Sum(sub_info_data))
 }
 key := company+"-"+fullname+"-"+timestamp
  getState, err := APIstub.GetState(key)

 if bytes.Equal(getState,[]byte("")) {
  test := Test{company, fullname,
                timestamp, hash_slice}
  testAsBytes, marshalErr :=
                json.Marshal(test)
  putErr := APIstub.PutState(
                fullname, testAsBytes)
  fmt.Println("Added new test: ", test)
  return shim.Success([]byte(fmt.Sprintf(
   "Successfully added %s test", key )))
 }
 return shim.Error("Error:
  key already exists.")
}
```

Fig. 4 presents performance results related to the creation of a single transaction by modifying the amount of hash values each transaction contains in the [2–10] range. Overall, achieved performance results show that a single transaction requires about 1.66 s (Fig. 4, left y-axis), without any relevant variation while varying the amount of hash values from 2 to 10. In fact, the computation of a single hash value takes less than 1 ms, thus much lower than the overall time required for the creation of the transaction. Of course, by increasing the amount of hash values per transaction the size of each transaction increases, starting from 5688 bytes in case of 2 hash values up to 6158 bytes with 10 hash values (Fig. 4, right y-axis). Overall, achieved performance results demonstrate that BlockHealth is scalable in relation to the amount of hash values, since it does not present relevant performance degradations.

Fig. 5 focuses on the performance while varying the frequency of generated transactions with a fixed amount of ten

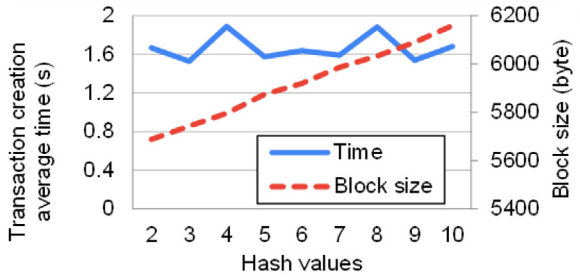
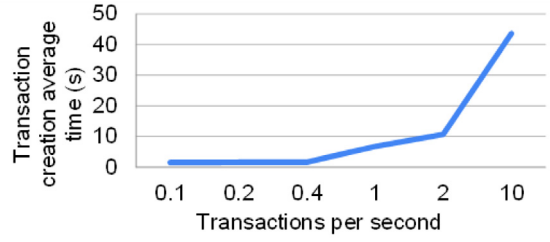
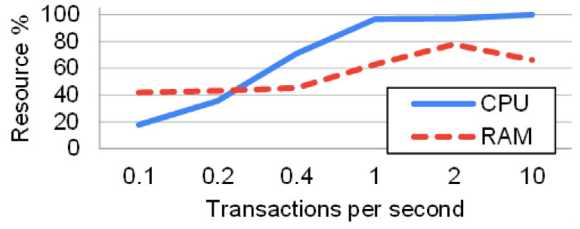


Fig. 4. Transaction creation time (left) and block size (right) of a single transaction with increasing amount of hash values.



(a) Average transaction creation time.



(b) CPU and RAM consumption.

Fig. 5. Transaction performance at increasing frequency with ten hash values.

hash values per transaction. As long as the amount of transactions per second is equal to or lower than 0.4 (thus consecutive transactions are generated with a period of at least 2.5 s, 24 transactions per minute) the BlockHealth solution demonstrates to be very efficient, with an average transaction time lower than 2 s (Fig. 5(a)) while not saturating the consumption of CPU and memory (Fig. 5(b)). However, when there are more than 1 transaction per second CPU and memory resources saturate and the time required to generate a transaction sharply increases up to 43 s.

3.3. Discussion

As clearly demonstrated by performance results presented above, the BlockHealth solution successfully achieves the objective of supporting the collection and sharing of health test data among companies. In particular, let us note that presented performance results greatly stress the proposed solution. In fact, the typical frequency a company posts new personal health data is much lower than the tested ones. Moreover, we have tested our BlockHealth prototype on top of a node with low/medium CPU and memory capabilities. Thus, achieved performance results confirm that the BlockHealth solution scales in relation to the amount of computed and stored hash values, with limited impact on its performance.

However, we recognize that a possible weakness of the proposed BlockHealth solution is it is not suitable in case of very high amount of generated information. In fact, while hardware specifications of nodes running the BlockHealth solution can be improved, performance of the Blockchain technology in general (and of Hyperledger Fabric in particular) are very far from the thousands of transactions per second a regular Web application can handle. Thus, its adoption must be focused on use cases generating a reduced amount of information per day and actually requiring a high level of security and availability together with the right to be forgotten, such as in case of health data sharing. To this purpose, note that a standard virtual machine is already enough for most of the cases, with up to 24 new personal health data submitted every minute (much more than the amount of health data we expect a company is able to generate).

Finally, the complexity and novelty of the Blockchain technology can represent a limit for the adoption of the BlockHealth solution. In fact, many companies can perceive the Blockchain as a complex technology difficult to deploy and time-consuming to maintain. To make easier the adoption of BlockHealth by all companies that are willing to use it, there is the need of providing snapshots of pre-configured and ready-to-run virtual machines or containers already containing required software modules. In this manner, even companies that do not have a strong IT department can access the BlockHealth solution in an easy-to-use manner. Finally, on the basis of the legislation applicable to each specific use case BlockHealth will require to support, there will be the need of providing detailed guidelines (provided by legal professionals) containing indications of best practices to be adopted to ensure the most effective use of the Blockchain technology in compliance with national and regional rules regarding the protection of personal data.

4. Related work

The Blockchain has been recently adopted in several real-world use cases to support secure sharing of information among interacting actors. For instance, [6] proposes to adopt Blockchain to avoid chargeback frauds. One of the typical target environments is the supply chain, pushed by the Blockchain capability of logging events in a distributed and secure manner without requiring any trusted centralized authority while supporting tracing, tracking, and business transactions [7–10]. In particular, [11] and [12] present a solution adopting the Blockchain to support servitization of ice cream machines, by exploiting smart contracts to ensure the validity of data related to machine usage. To ensure privacy among different business competing actors (e.g., suppliers of ice cream ingredients), information about the amount and type of produced ice creams are stored in per-supplier ledgers. Interested readers can refer to [13] for a survey of recent state-of-the-art contributions exploiting Blockchains to increase efficiency, reliability, and transparency of the supply

chain. Finally, [14] presents a comparison among permissioned blockchain frameworks adopted in industrial environments.

The spread of the Blockchain has pushed the focus on its capability of ensuring the privacy of involved actors [15,16]. For instance, the Blockchain-based ID as a Service (BIDaaS) solution [17] supports the mutual authentication among actors without requiring to share among them any pre-shared information or security credential. [18] exploits the Blockchain to ensure data privacy of IoT devices by exploiting smart contracts to validate connection rights based on predefined privacy permission settings and on the availability, for IoT devices, of a set of stored of known misbehaviors. [19] exploits the Blockchain in IoT-aided Smart Homes to support a privacy-preserving transactive energy management solution. In particular, the proposed solutions is based on a distributed algorithm to optimize energy management while not revealing users' private information.

By focusing on healthcare management solutions, recent research efforts demonstrate the huge interest in exploiting the Blockchain to manage and share health data. In particular, the survey proposed in [20] outlines that data sharing, access control, and audit are some of the most important functional use cases the Blockchain is adopted for in the healthcare sector. Moreover, it stresses that limited scalability, low performance, and high complexity represent primary issues that reduce the applicability of the Blockchain for healthcare. [21] presents a solution allowing to share health data while ensuring that the individual the data is related to is aware of it. In particular, a smart contract is exploited to automate the enforcement of a generic consent model, thus ensuring not only that individual consent is respected but also that every actor sharing data is accountable. Finally, [22] ensures fine-grained access control to health data in the Blockchain by adopting an Attribute-Based Encryption (ABE) solution. The main idea is to store every personal health information in the Blockchain but encrypted exploiting the ABE mechanism, a one-to-many public key cryptographic primitive. In this manner, while every actor able to access the Blockchain can retrieve encrypted personal health data, only actors with decryption key can actually access plain health data.

5. Conclusions

The paper presented the BlockHealth solution, originally adopting Blockchain to support a distributed clinical test register, shared among different companies. In particular, each company can access the Blockchain to retrieve the hash value of shared personal health data, with the goal of verifying that previously health data stored in private databases have not been modified after their insertion in the system. In this manner, BlockHealth achieves a proper trade-off between personal health data protection and data sharing to ensure employee safety, in line with state-of-the-art legislation trends. Achieved results based on a working prototype exploiting Hyperledger Fabric demonstrate not only the feasibility of the proposed solution, but also its efficiency. Based on encouraging performance results, we intend to extend our prototype by testing it with several companies interacting within the same supply chain interested in sharing health data of their employees.

CRediT authorship contribution statement

Eugenio Balistri: Methodology, Software, Validation, Investigation, Data curation, Writing - review & editing. **Francesco Casellato:** Methodology, Software, Validation, Investigation, Data curation, Writing - review & editing. **Carlo Giannelli:** Conceptualization, Data curation, Writing - original draft, Supervision, Project administration. **Cesare Stefanelli:** Conceptualization, Writing - review & editing, Supervision, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

Partially funded by POR-FESR Emilia Romagna 2014–2020, "SmartChain: interoperable and efficient systems for the secure management of industrial supply chains" project.

References

[1] European Parliament and Council of European Union, Regulation (EU) 2016/679, 2016, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[2] S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System, 2008, Available online at https://bitcoin.org/bitcoin.pdf.

[3] D.J. Yaga, P.M. Mell, N. Roby, K. Scarfone, Blockchain technology overview, in: NIST Interagency/Internal Report (NISTIR) - 8202, 2018.

[4] M. Belotti, N. Božić, G. Pujolle, S. Secci, A vademecum on blockchain technologies: When, which and how, IEEE Comm. Surveys & Tutorials (2019).

[5] Hyperledger Fabric: A Blockchain Platform for the Enterprise, Available online at https://hyperledger-fabric.readthedocs.io/en/release-2.3/.

[6] D. Liu, J.H. Lee, CFLedger: PReventing chargeback fraud with blockchain, ICT Express (2021).

[7] K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, Blockchain-based soybean traceability in agricultural supply chain, IEEE Access 7 (2019).

[8] M.I.S. Assaqty, et al., Private-blockchain-based industrial IoT for material and product tracking in smart manufacturing, IEEE Netw. 34 (5) (2020) 91–97.

[9] W. Alkhader, N. Alkaabi, K. Salah, R. Jayaraman, J. Arshad, M. Omar, Blockchain-based traceability and management for additive manufacturing, IEEE Access 8 (2020).

[10] H. Patel, B. Shrimali, AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology, ICT Express (2021).

[11] E. Balistri, F. Casellato, C. Giannelli, R. Lazzarini, C.F. Ngatcha Keyi, C. Stefanelli, Servitization in the Era of Blockchain: the Ice Cream Supply Chain Business Case, in: 2020 Int. Conf. on Technology and Entrepreneurship (ICTE), Bologna, Italy, 2020, pp. 1-8.

[12] A. Biscotti, et al., Internet of Things and Blockchain Technologies for Food Safety Systems, in: 2020 IEEE International Conference on Smart Computing (SMARTCOMP), Bologna, Italy, 2020, pp. 440-445.

[13] G. Perboli, S. Musso, M. Rosano, Blockchain in logistics and supply chain: A lean approach for designing real-world use cases, IEEE Access 6 (2018).

[14] J. Polge, J. Robert, Y. Le Traon, Permissioned blockchain frameworks in the industry: A comparison, ICT Express 7 (2) (2021).
[15] R. Henry, A. Herzberg, A. Kate, Blockchain access privacy: Challenges and directions, IEEE Secur. Priv. 16 (4) (2018) 38–45.
[16] J. Bernal Bernabe, J.L. Canovas, J.L. Hernandez-Ramos, R. Torres Moreno, A. Skarmeta, Privacy-preserving solutions for blockchain: Review and challenges, IEEE Access 7 (2019) 164908-164940.
[17] J. Lee, BIDaaS: Blockchain based ID as a service, IEEE Access 6 (2018) 2274–2278.
[18] F. Loukil, C-. Ghedira-Guegan, K. Boukadi, A.N. Benharkat, E. Benkhelifa, Data privacy based on IoT device behavior control using blockchain, ACM Trans. Internet Technol. 21 (23) (2021) 1.
[19] Q. Yang, H. Wang, Privacy-Preserving Transactive Energy Management for IoT-aided Smart Homes via Blockchain, IEEE Internet of Things J., http://dx.doi.org/10.1109/JIOT.2021.3051323, in press.
[20] E. Chukwu, L. Garg, A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations, IEEE Access 8 (2020) 21196–21214..
[21] V. Jaiman, V. Urovi, A consent model for blockchain-based health data sharing platforms, IEEE Access 8 (2020) 143734-143745.
[22] A.E.B. Tomaz, J.C.D. Nascimento, A.S. Hafid, J.N. De Souza, Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain, IEEE Access 8 (2020) 204441-204458.