A Blockchain Architecture for the Italian EHR System

Mario Ciampi, Angelo Esposito, Fabrizio Marangio, Giovanni Schmid, Mario Sicuranza
Institute for High Performance Computing and Networking
National Research Council of Italy
Via Pietro Castellino, 111 – 80131 Naples, Italy
e-mail: {mario.ciampi, angelo.esposito, fabrizio.marangio, giovanni.schmid, mario.sicuranza}@icar.cnr.it

***Abstract*—In the last years, significant changes of important socio-economic indicators, like population growth, life expectancy increase and patient mobility, have implied the need to provide new models for health provision. Thus, several efforts have been done to adequate and evolve the current e-health systems for enabling them to gather patient health data produced by health facilities in an interoperable way and according to shared business processes. However, even if such systems are now starting at collecting health data, it is still not possible to verify that all the tasks of a specific process are correctly executed. This work presents a permissioned blockchain architecture designed to manage the Electronic Health Records of the users, able to track the operations performed by the actors involved in a health process. The architecture proposed is compliant with both the Italian Regulation on Electronic Health Record and the recently introduced GDPR. A proof-of-concept of the architecture has been developed and validated against a relevant use case.**

Keywords-EHR; blockchain; patient-centric; architecture.

I. INTRODUCTION

An increasingly important problem for the well-being of modern societies is to have efficient, reliable and scalable health support systems. This is necessary to provide adequate healthcare – in the medium and long term – to populations whose lifetime expectation tends to increase constantly, but whose individuals often do not have a satisfactory health state, especially during their old age. Realizing these systems is an essential condition for containing public spending and the sustainability of national health systems. Indeed, they can be used to prevent health diseases, through the lifestyle monitoring of people and the use of innovative and non-invasive therapies based on precision medicine. In the attempt to achieve this goal, huge efforts are underway in EU countries to digitize health processes for increasing usability and reliability for patients and healthcare personnel, allowing for a reduction in time and costs. The areas in which improvements can and must be achieved are still many, and the margins of enhancement allowed by emerging technologies like permissioned blockchains for the secure and transparent processing of distributed workflows can be really substantial, such as to revolutionize prevention and treatment approaches. Indeed, current systems are rooted on data producers (e.g., hospitals and healthcare companies), while infrastructures and protocols designed to guarantee their adequate interoperability and a "patient-centric" approach are lacking, if not completely absent. This complicates and makes healthcare costlier for citizens, as well as favoring the incidence of accidental errors and frauds, often with serious consequences in terms of public health.

In this work, we propose a blockchain-based network for the decentralized management of Electronic Health Records (EHR), specifically designed according to the Italian EHR interoperability architectural model. We have developed a proof-of-concept prototype and performed a set of simulations for showing the effectiveness of our design and the advantages of deploying our system for the Italian National Health Service (NHS).

A. The Italian public health service

The Italian NHS is a system of facilities and services that have the purpose of guaranteeing all citizens, under conditions of equality, universal access to the equitable provision of health services. The Italian Constitution provides for legislative protection of the State and the Regions for the protection of health. The State determines the *essential levels of assistance* that must be guaranteed throughout the national territory, while the Regions plan and manage health care in their area in full autonomy [1].

In the last decade, many efforts have been made by national and regional institutional and technical organizations with the aim of improving the quality of health services and reducing costs by applying information and communication technologies in healthcare. The most relevant efforts concern the design and implementation of Health Information Systems (HISs) [2], with particular reference to the EHR, which has the aim of collecting all the health information related to a patient produced by the healthcare facilities and services on the national territory [3].

In order to overcome the problem of interoperability among the different regional EHR systems, the emanation of specific Italian norms since 2012 has allowed the competent Institutions (Agency for Digital Italy, Ministry of Health, Ministry of Economy and Finance, with the technical support of the National Research Council of Italy) defining the national EHR interoperability architectural model. This model is based on 21 regional IT platforms that interact each other by means of a national framework, namely National Interoperability Infrastructure (INI), as shown in Figure 1.

 ISBN: 978-1-61208-759-7

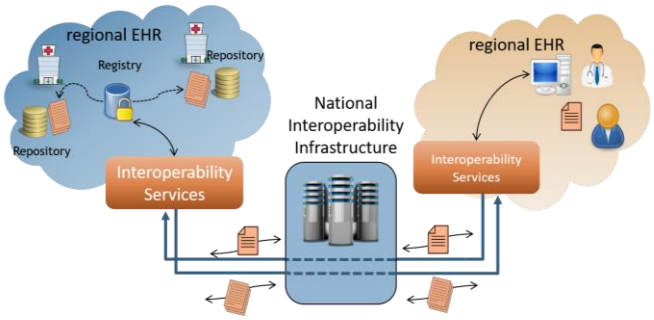

Figure 1. Italian EHR Interoperability Framework.

Each regional IT platform has the aim of indexing into a regional registry the metadata of the health digital clinical data related to its patients, whereas such data are stored into the data repositories managed by the health facilities [4].

The national interoperability infrastructure is conform to the registry/repository paradigm based on the IHE XDS Integration profile, which has the scope of facilitating the sharing of patient EHRs across health enterprises within an affinity domain (a group of healthcare facilities that intend to work together) [5]. With regards to the data structure, it is necessary to distinguish between clinical data and metadata. Clinical data are structured according to the HL7 CDA Rel. 2.0 standard format [6]. Such a format consists of two main sections: *header*, which contains context data (like patient name, author, etc.); *body*, which contains the clinical content. Each type of clinical document is structured according to Italian Implementation Guides, which are national localizations of the HL7 CDA Rel. 2 standard. It is worth noting that also clinical data represented in PDF are accepted by the national interoperability infrastructure. Metadata are a set of attributes related to the clinical data, which have the aim of facilitating their indexing and retrieval. Such metadata contain information like patient identifier, author, document reference and so on. They can easily be mapped to the data contained in the header of the HL7 CDA Rel. 2.0 documents. The structure and the types of the metadata comply with the IHE XDS profile. Moreover, a set of interoperability business processes have been formalized in order to specify all the activities performed by each actor involved. Such processes describe the steps to index, search for, and retrieving patient health data, wherever they are memorized on the national territory. All the platforms expose a regional node, which acts as an interface among the internal subsystems and the other regional nodes. The interactions among the regional nodes, based on consolidated international health informatics standards, are mediated by INI.

Along with the architectural model and the business processes, the functional and privacy requirements, as well as the technical specification for assuring interoperability have been defined [7]. Nowadays, almost all the regional EHR systems are able to i) collect patient health data, ii) permit their consultation to all the authorized actors (health professionals and operators, patients, caregivers, etc.), and iii) interact with other regional EHR systems to exchange information.

B. *Current issues and trends*

Despite the efforts made so far to develop a national federated architecture for the interoperability of EHR systems in Italy, significant actions are still to be taken in order to ensure an effective and correct implementation of the health business processes. In more detail, each business process is composed of a set of activities, part of which are performed by a regional EHR platform inside a Region and the other part of them is executed outside the Region by means of the interactions between a regional node and INI. Currently, the last one permits to control and track all the requests coming from the EHR platforms, whereas the interactions occurred within a Region are logged by the regional system. For these reasons, at the moment it is not possible to control that all the activities of a specific process are correctly executed, unless to analyze all the event logs generated by the distributed systems involved. Moreover, even considering a regional context, the operations performed are often tracked by different subsystems, not allowing this way the possibility to certify that the tasks executed are compliant to the desired workflows.

The definition of a security architecture, able to store in a reliable and effective way all the operations executed and easily integrable with the national architectural model, would allow ensuring patients, health professionals, and government organizations that the health data of interest are produced according to the specified and shared procedures. Such an architecture, proposed in this paper, would permit also the patients to: i) specify the policies for accessing their health data in a more flexible way, and ii) verify all the access requests performed by unauthorized users.

The rest of the paper is organized as follows. Section II describes relevant related works. Section III presents our contribution, giving the system requirements and its core architecture. Section IV provides details on the prototype developed, whereas Section V concludes the paper.

II. RELATED WORKS

In the last years, a massive amount of academic and industry work has been devoted to blockchain technologies and their applications in various sectors besides fintech. Healthcare, alongside with the supply-chain industry, has probably one of the highest prospects on opportunities from these technologies. A search for the term “blockchain” on PubMed returned 16 results in 2017, 77 results in 2018, and 88 results in the first eight months of 2019. Various companies have already implemented or are working on putting a blockchain system to the test for a healthcare use case (e.g., [8]-[12]), and as for July 2019 there are seven major healthcare blockchain consortia [13].

Below, for the sake of brevity, we will limit our discussion to three major projects, which have resulted in working implementations. Indeed, they exploit different and significant approaches to the management of EHRs that have influenced our work.

 ISBN: 978-1-61208-759-7

MedRec [14] is a project initiated in 2016 by MIT Media Lab and Beth Israel Deaconess Medical Center, with the aim to overcome four important issues in the healthcare context: fragmented data, slow access to medical data, systems interoperability, and patient agency. It provides a decentralized approach in which the permissions, data storage location, and audit logs are maintained in the blockchain, while all healthcare information remains in the already pre-existing EHR systems. The project has developed two blockchain platforms both built on Ethereum's technologies, but with major differences. Version 1.0 [15] was a small-scale, private network with specific APIs, whilst the current version 2.0 [16] is developed using Go-ethereum (Geth) and Solidity, but with changes to the amount of information stored on the blockchain for improving the scaling and privacy properties of transactions. Other major differences concern the consensus and governance protocols. MedRec 1.0 uses the Ethereum's proof-of-work protocol with appropriate parameters, where the mining process would be performed by medical researchers, who in turn would gain access to aggregated and anonymized data useful to further medical research. However, this approach poses concerns about the security and governance of patient data. In the current version, therefore, the EHR providers maintain the blockchain, resulting in a small and closed set of nodes that can reach consensus without the cost of mining. Providers use a proof-of-authority to append new blocks, and also to determine who is in their group.

Patientory [8] is both the name of a digital health company established in 2015, and a no-profit association for developing and governing the PTOYNet [16] blockchain. PTOYNet is a fork of Quorum, which in turn is an enterprise-focused version of Ethereum mainly by developers of JPMorgan Chase. Quorum executes smart contracts within the Ethereum Virtual Machine, but uses alternatives to the mining-based consensus protocol of Ethereum; moreover, it has built-in the feature of transaction confidentiality thanks to end-to-end encryption. PTOYNet has been adapted from Quorum in order to store healthcare records and manage their transactions through the PTOY token, providing an ecosystem for healthcare organizations to collaborate and innovate in a completely decentralized fashion. In exchange for PTOY, patients and healthcare organizations are able to use the network to rent health information storage space and execute health-specific smart contract payments and transactions. Patientory Inc. gains its revenue from the Software as a Service (SaaS) annual contract, as well as population health management services from the aggregation of data on the platform: machine learning physician diagnoses support, patient-provider UIcare coordination, and patient engagement. In 2018 the company launched on the market a mobile distributed application (DApp) which leverages the services offered by the PTOYNet platform. At the time of writing, the approximate return on investment (ROI) in PTOY if purchased at the time of launch is -98.84% [17].

Medicalchain [10] is an infrastructure to securely store and share EHRs: any interactions with EHRs are recorded as transactions on the network, but the EHRs are encrypted and stored in data stores within appropriate regulatory jurisdictions. Its first implementation was released in February 2018 and is built on a double blockchain. The first blockchain is a permission-based Hyperledger Fabric architecture, which allows varying access levels to the EHRs: users can control who can view their records, how much they see and for what length of time. The second blockchain is Ethereum, which is used to run all the applications and services for the Medicalchain platform through the ERC20-compliant cryptocurrency token MedToken (MTN). MTNs have been offered through an initial coin offering (ICO) crowd selling process started on February 1st 2018. At the time of writing, Medicalchain has a current supply of 500,000,000 MTN with 308,656,962 MTN in circulation, with an approximate ROI of -98.49% [18].

The previous examples should point out the difficulties of realizing a blockchain-based EHR management system, both in terms of technical deployment and governance. These difficulties are exacerbated by the EU regulations in different ways. For example, the storage of EHRs in the ledger is not only inappropriate since blockchain systems do not have the requisites of massive databases, but it makes very difficult to enforce the right to data modification or erasure under particular circumstances, as stated by Articles 16 and 17 of the General Data Protection Regulation (GDPR) [19]. More generally, blockchains underline the challenges of adhering to the requirements of data minimization and purpose limitation in the current form of the data economy.

III. OUR CONTRIBUTION

We are working on a blockchain system for the EHR management compliant with both the recently introduced GDPR and the national EHR interoperability architectural model described in Section I.A. Indeed, our design centers around the functional requirements listed in Tables I, II and III. These requirements stem from the framework of fundamental rights of the GDPR, and the organizational constraints for the national EHR interoperability architectural model. They can be grouped into those deriving from needs related to patients and those arising from the needs of health organizations.

Patients' needs are related to their privacy and the rights to data access (Article 15 GDPR) and data portability (Article 20 GDPR), which provide patients with control over what others do with their personal data and what they can do with that personal data themselves.

 ISBN: 978-1-61208-759-7

TABLE I. REQUIREMENTS FOR PATIENTS

P1	Patients should have the right of control over their data on system. They must be able to specify who can do what on their own data
P2	Patients should have the ability to change at any time the access rights to their data
P3	Patients must be able to hide their data from specific healthcare practitioners
P4	Patients need to have the ability to know how and when their data are accessed and for which purpose. This will be possible through the *disclosure* property, as indicated in the EU directives. Patients should be able to provide access to healthcare practitioners that are not entitled to access their data
P5	Patients must be able to research and retrieve their health data in the system

TABLE II. REQUIREMENTS FOR HEALTHCARE ORGANIZATIONS

O1	The data holder must be the healthcare organization which generated data
O2	Healthcare organizations must provide protection to the data they hold. Every healthcare organization can manage security policies with a certain level of autonomy
O3	Every healthcare organization should be able to design its own security policy and to enforce it. The definition of the access policies must be implemented in total freedom and through a highly flexible mechanism
O4	Healthcare organizations should be able to change quickly and easily the access policies of a given document
O5	The access control should not add a significant administrative overhead
O6	Audit operations are required: it is necessary to track all the operations carried out by a healthcare organization

TABLE III. ADDICTIONAL REQUIREMENTS

A1	Identification and authorization of the actors' functions
A2	Document indexing functions: the Healthcare Assistance Region of the patient has the responsibility of maintaining index metadata related to all the documents related to its patients, even if such documents are produced and maintained by health facilities sited outside the Region
A3	Research and recovery of health data functions related to a specific patient
A4	Search and retrieval mechanisms and pseudo-anonymization data functions
A5	Backup and restore functions
A6	Functions for allowing a patient to send data produced by certified devices to organizations accredited to the blockchain for storage and management

A. System overview

Our system is a kind of permissioned network where, according to recent blockchain design principles [20], nodes are organized in *users*, *validating*, *endorsers*, and *ordering*.

- Users are just nodes which require services by submitting transactions, and in our context are patients, physicians and other personnel of the healthcare sector.
- Validating nodes have their own copy of the ledger: they are healthcare-related companies and institutions that check for transaction I/O versus the current status of the ledger.
- Endorsers are validating nodes which, on the basis of a consensus policy provided at the application layer, have got the additional task of checking transaction correctness both syntactically and by running them.
- Ordering nodes are nodes that – through a suitable consensus protocol for the ledger layer, implemented in a dedicated module – have to assemble transactions in blocks and select the next block of the chain for the relevant blockchain.

Ordering nodes do not need to store any blockchain, nor they are aware of transaction contents. They just assemble the endorsed transactions received in blocks and communicate the next block to the validating nodes for the relevant blockchain via a gossiping protocol.

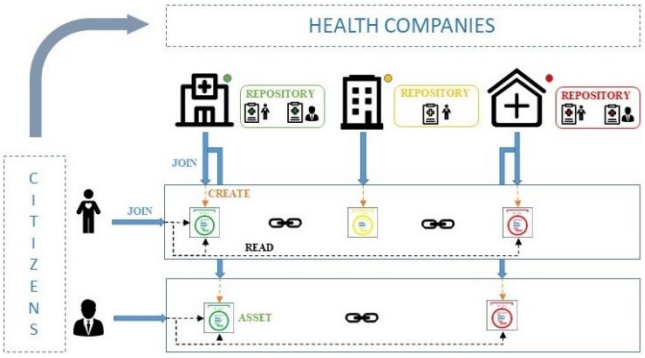

Figure 2. An high level view of our architecture.

Our system allows overcoming the current issues for the national interoperability of EHR systems in Italy. Indeed, the blockchain functionalities allow to have corroborate evidence that all the activities related of a specific process are correctly executed, provided that these activities are coded as appropriate transactions. The core architecture of our system is illustrated in Figure 2. It makes use of the building blocks described in the following sections.

B. Participants

We have identified the following four types of participants:

- *Patient*: any EU citizen, or any non-EU citizen with a valid permit to stay or a residence card.
- *Company*: any public health company, or any private health company authorized by the Ministry of Health.
- *Admin Officer*: an administrative official in charge of patient registration and accounting for a health company.
- *Company Doctor*: a physician working in a company registered in the network, who is in charge of carrying out diagnostic examinations or medical reports for patients, thus creating their health data.

Participants are created in a hierarchical way:

- Patients and Companies provide their info in order to be registered in the system.
- Companies create their own Admin Officers.
- Admin Officers of a given company create both the company's users (patients) and the physicians.

Patients get access to the system thanks to one of the two authentication methods prescribed in the National Interoperability Infrastructure, which are SPID or CNS. SPID [21] is the unique system of access with digital identity to the online services of the Italian Public Administration. CNS [22] is a device (i.e., a Smart Card or USB stick) that contains a "digital certificate" of personal authentication. They are identified by their *fiscal codes* (CF) (identify individuals and companies in Italy), and represented by

 ISBN: 978-1-61208-759-7

objects like that illustrated in Figure 3. Similar data structures are provided for admin officers and physicians.


```
{
  "$class": "org.electronic.health.record.Patient",
  "birthDate": "08-10-1987",
  "birthPlace": "Napoli",
  "age": 32,
  "companyList": [],
  "address": {
    "$class": "org.electronic.health.record.Address",
    "state": "Italia",
    "region": "Campania",
    "city": "Napoli",
    "houseNumber": "24",
    "street": "Via Roma",
    "zipCode": "80100"
  },
  "CF": "ALFDRS87D08F839L",
  "name": "Alfio",
  "surname": "Dorsi",
  "phone1": "3478123156",
  "email": "alfio.dorsi@gmail.com"
}
```


Figure 3. Example of Patient.

C. Assets

According to the national EHR interoperability architectural model described in Section I.A, patient health data are stored and accessed through the regional EHR systems. The patient's blockchain manages and stores just the transactions that produce or consume the patient's registration and authorization information and their health data. Specifically, each health document is represented in the patient's blockchain as an asset containing the link to the actual anonymized document, plus a set of metadata encoding the majority of fields described in the national technical specification for EHR interoperability [5]. Some of the fields specified in our assets are:

- *authorPerson:* defines the *CF* identifier of the author, in our case the physician that created the asset.
- *authorRole:* defines the role of the author (like physician of general medicine).
- *authorInstitution:* defines the *CF* identifier of the company in which the physician who created the asset works.
- *patientID:* the *CF* identifier of the participant for whom the document is created.
- *classCode*: defines the class of the document (prescription - PRS, medical report – REF, and so on).
- *confidentialityCode:* defines the level of confidentiality of the asset (unrestricted, low, moderate, normal, restricted, very restricted).
- *mimeType;* identifies the MIME type of the indexed document [5].

In Figure 4, we show an example of asset. As we can note, some fields are not filled. They are indeed optional fields that are automatically or manually filled only if necessary.


```
{
 "$class": "org.electronic.health.record.Doc",
 "docId": "d16e7",
 "creationDate": "2019-07-30T07:08:20.815Z",
 "authorPerson": "RSSDVD65D15F839N",
 "authorRole": "MMG",
 "authorInstitution": "Centro Diagnostico Radium",
 "XDSDocumentEntry_ClassCode": "WOR",
 "XDSDocumentEntry_Comments": "",
 "XDSDocumentEntry_ConfidentialityCode": "N",
 "XDSDocument_EntryFormatCode": "Prescrizione",
 "XDSDocumentEntry_eventCodeList": "P99",
 "XDSDocumentEntry_healthcareFacilityTypeCode": "Ospedale",
 "XDSDocumentEntry_mimeType": "text_x_cda_r2_xml",
 "XDSDocumentEntry_mimeTypePracticeSettingCode": "AD_PSC001",
 "XDSDocumentEntry_Title": "",
 "XDSDocumentEntry_TypeCode": "Prescrizione_farmaceutica",
 "patientCF": "DRSLSN87A13F839Z",
 "docType": "",
 "companyId": "CDRAD",
 "readAccess": [
   "PCCFRC00D03F205L"
 ],
 "hash": "",
 "dimension": "",
 "compDoctor":
"resource:org.electronic.health.record.CompanyDoctor#RSSDVD65D15F8
39N",
 "company": "resource:org.electronic.health.record.Company#CDRAD",
 "patient":
"resource:org.electronic.health.record.Patient#DRSLSN87A13F839Z"
}
```


Figure 4. Example of Asset.

D. Transactions

Transactions define the logic for the creation and updating of participants and assets. They are articulated in the following four sets, depending on their scope:

- *Creation and modification of participants*: various transactions permit to authorized parties to create and modify individual participants. Participants are univocally identified in the system by their fiscal code, which can be set and modified only by the creator of the participant, following the rules given in Section III.B. Some other types of data, like addresses or phone numbers, can be inserted or modified by the participants themselves after their creation. The whole process is managed through suitable *create* and *update* ACLs related to participants.
- *Creation and modification of assets*: consistently with the fact that assets represent patient's health data in the ledger, only agents (e.g., physicians, medical devices) previously authorized by a patient can create or update their assets. Only the creator of an asset can subsequently modify it, but in any case, this will be tracked in the ledger through a suitable transaction. By default, assets can be read by the patients to which they refer to and by their *general practitioners*, other than by their creators. If needed, the patient can give read access for the document to other participants in the network through a specific transaction, as detailed below. The creation, update

 ISBN: 978-1-61208-759-7

and access of assets are regulated by namesake transaction sets.

- *Access to documents*: this kind of transactions implements the P4 requirement of disclosure (see Section III.A) and are regulated by specific *read* ACLs.
- *Access to personal info*: patients must give their explicit consent to other participants (e.g., healthcare companies) for reading their personal information. This kind of transactions implements requirement P1 and are regulated by other *read* ACLs.

IV. IMPLEMENTATION AND RESULTS

We have implemented a prototype of a permissioned blockchain network, in order to assess – through a set of use case simulations – the proposed architecture against the functional requirements indicated in Section III. To implement our network, we used Hyperledger Composer v0.20.8 [23] and Hyperledger Fabric v1.2 runtime [24]. All our simulations have been performed on a Virtual Machine running Ubuntu 16.06.6 LTS. To test our architecture, we installed *composer-cli v.0.20*, *composer-rest-server v.0.20*, *generator-hyperledger-composer v.0.20*, *Yeoman* and *composer-playground v.0.20*.

In the following, we describe the use case where a general practitioner has prescribed an examination to a patient, as an illustrative example of a set of workflows that, thanks to the proposed architecture, are compliant to the requirements given in Section III. In the following images, the identifiers related to patients and health authorities are circled in red, so as to be able to identify the actors involved.

First, as shown in Figure 5, a company tries to access patient data. The system returns an error because the company has not the rights to read the patient's data. Therefore, as shown in Figure 6, the patient has to give the access to her/his personal information to the previous company; without this explicit consent, nobody can see her/his profile in the blockchain.

After the acceptance of the patient's request by a company admin officer, the company will be able to access to the patient's personal information (see Figure 7). This way, the request submitted (via a transaction not shown here) by the patient's general practitioner can be processed by the health company, which will reserve an examination date and will assign a specialist physician for the patient.

On the day of the examination, the physician will create the related asset by entering the required data (Figure 8), and such asset can be accessed read-only by the patient and her/his own general practitioner. No one can access the asset other than its creator, the patient and her/his general practitioner (Figure 9).

The patient can give read-only access to the document to other participants in the blockchain network (Figures 10 and 11); after that, they are allowed to read the asset. It is worth to stress here that only the patient has this capability, which correspond to the disclosure property P4.

The previous example and the other simulations we performed during our experimental tasks show that our blockchain network manages patient's data so to satisfy requirements P1-P5. Notice that our network manages assets that, as detailed in Section III.D, are composed of a set of metadata encoding the majority of fields described in the national technical specification for EHR interoperability, plus a link to get access to the actual anonymized health document provided for the patient. The patient's health document is not stored in the blockchain network, but in the data repository of the health company that produced it (see Figure 2). This way, our architecture satisfies requirements O1-O6 without sacrificing the audit requirement O6, often failed in current implementations. Last but not least, blockchain native functionalities allow to satisfy the requirements A1-A6.

```
To restart the REST server using the same options, issue the following command:
   composer-rest-server -c CDRAD@electronic-health-record -n never -u true -w tr
ue
Web server listening at: http://localhost:3000
Browse your REST API at http://localhost:3000/explorer
Unhandled error for request GET /api/Patient/DRSLSN87A13F839Z: Error: Unknown "P
atient" id "DRSLSN87A13F839Z".
```

Figure 5. A Company identified with ID CDRAD cannot see the patient identified by the ID DRSLSN87A13F839Z without her/his permission.

```
                -VirtualBox:~/fabric-dev-servers/electronic-health-record$ comp
oser transaction submit -c DRSLSN87A13F839Z@electronic-health-record -d '{
>   "$class": "org.electronic.health.record.GiveReadAccess",
>   "companyList": "CDRAD",
>   "pat": "resource:org.electronic.health.record.Patient#DRSLSN87A13F839Z"
> }'
Transaction Submitted.

Command succeeded
```

Figure 6. The patient DRSLSN87A13F839Z gives the read access to her/his information to the company.

```
                -VirtualBox:~/fabric-dev-servers/electronic-health-record$ curl
 -X GET --header 'Accept: application/json' 'http://localhost:3000/api/Patient/D
RSLSN87A13F839Z'
{"$class":"org.electronic.health.record.Patient","birthDate":"13-01-1987","birth
Place":"Napoli","age":32,"companyList":["NA204","CDRAD"],"address":{"$class":"or
g.electronic.health.record.Address","state":"Italia","region":"Campania","city":
"Napoli","street":"Via Toledo","houseNumber":"12","zipCode":"80132"},"CF":"DRSLS
N87A13F839Z","name":"Alessandro","surname":"De Rosa","phone1":"0815443121","emai
l":"alessandro.derosa@gmail.com"}                -VirtualBox:~/fabric-dev-serve
```

Figure 7. Making a curl operation on the REST server: the Company with ID CDRAD can now read patient's personal information.

```
                -VirtualBox:~/fabric-dev-servers/electronic-health-record$ curl
 -X GET --header 'Accept: application/json' 'http://localhost:3000/api/Doc/d16e7
'
{"$class":"org.electronic.health.record.Doc","docId":"d16e7","creationDate":"201
9-07-30T07:08:20.815Z","authorPerson":"RSSDVD65D15F839N","authorRole":"MMG","aut
horInstitution":"Centro Diagnostico Radium","XDSDocumentEntry_ClassCode":"WOR","
XDSDocumentEntry_Comments":"","XDSDocumentEntry_ConfidentialityCode":"N","XDSDoc
ument_EntryFormatCode":"Prescrizione","XDSDocumentEntry_eventCodeList":"P99","XD
SDocumentEntry_healthcareFacilityTypeCode":"Ospedale","XDSDocumentEntry_mimeType
":"text_x_cda_r2_xml","XDSDocumentEntry_mimeTypePracticeSettingCode":"AD_PSC001"
,"XDSDocumentEntry_Title":"","XDSDocumentEntry_TypeCode":"Prescrizione_farmaceut
ica","patientCF":"DRSLSN87A13F839Z","docType":"","companyId":"CDRAD","readAccess
":[],"hash":"","dimension":"","compDoctor":"resource:org.electronic.health.recor
d.CompanyDoctor#RSSDVD65D15F839N","company":"resource:org.electronic.health.reco
rd.Company#CDRAD","patient":"resource:org.electronic.health.record.Patient#DRSLS
N87A13F839Z"}                -VirtualBox:~/fabric-dev-servers/electronic-health
```

Figure 8. The physician which created an asset and can see the asset in the blockchain.

Figure 9. Only the physician which created the asset and the participant to which the asset refers to can access the data in blockchain. A participant identified with a different ID (PCCFRC00D03F205L) cannot see the asset.

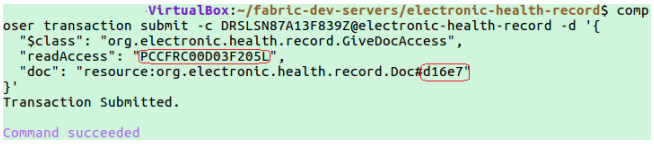

Figure 10. Patient with ID DRSLSN87A13F839Z can give read access permission to the participant with ID PCCFRC00D03F205L.

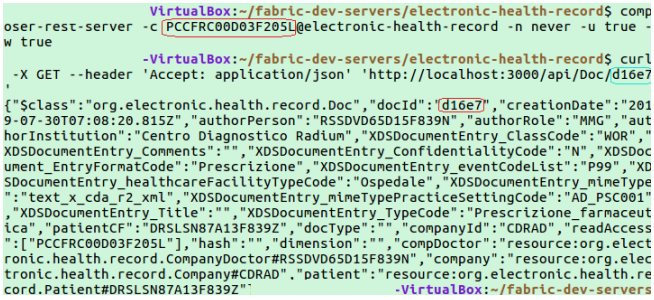

Figure 11. Now the participant with ID PCCFRC00D03F205L can read the document.

It is worth noting that some asset field values in Figure 4 (e.g., "Prescrizione") do not match the technical specification for EHR interoperability based on the IHE XDS framework. This is because of a current limitation of the Hyperledger Composer "Enumerated Types", which does not accept some special characters, e.g., the dot character. This issue can be overcome thanks to a lookup table processed at the application layer.

V. CONCLUSIONS AND FUTURE WORK

We have designed a blockchain-based architecture for the decentralized management of EHRs, which is compliant with the GDPR and allows to overcome some main issues concerning the current federated architecture for the national interoperability of EHR systems in Italy. Our proof-of-concept network represents just the core architecture of a federated EHR management system, and much more work is required to get a complete working system. First, our network has to be coupled with a suitable access control and security framework to protect patient's health data. This framework has to be designed according to the functional requirements illustrated in Section III, but it should compromise neither the usability of the system nor its scalability and management. Second, an accurate and full-fledged user interface has to be realized through the development of apps customized for the different kinds of network participants. Our next work will concern the design and implementation of the access control and security framework. Then we are going to realize a testbed for assessing the effectiveness of the EHR management system resulting by coupling it with the blockchain network illustrated in this work.

REFERENCES

[1] Italian Ministry of Health, http://www.salute.gov.it/portale/lea/dettaglioContenutiLea.jsp?lingua=italiano&id=5073&area=Lea&menu=vuoto, retrieved 09/2019.

[2] A.D. Black, J. Car, C. Pagliari, C. Anandan, K. Cresswell, T. Bokun, B. McKinstry, R. Procter, A. Majeed, and A. Sheikh, "The impact of ehealth on the quality and safety of health care: a systematic overview", PLOS Med. 8(1), 2011, pp. 1-16.

[3] F. Aminpour, F. Sadoughi, and M. Ahamdi, "Utilization of open source electronic health record around the world: a systematic review", Off. J. Isfahan Univ. Med. Sci. 19(1), 2014, pp. 57-64.

[4] M. Ciampi, M. Sicuranza, A. Esposito, R. Guarasci, and G. De Pietro, "A technological framework for EHR interoperability: experiences from Italy" Comm. in Computer and Information Science, Springer, 736, 2017, pp. 80-99.

[5] Integrating the Healthcare Enterprise, http://www.ihe.net/, retrieved 09/2019

[6] HL7 Version 3 Clinical Document Architecture (CDA) Release 2, https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7, retrieved 09/2019.

[7] Agency for Digital Italy of the Presidency of the Council of Ministers, https://www.fascicolosanitario.gov.it/, retrieved 09/2019.

[8] https://patientory.com/technology/, retrieved 09/2019.

[9] https://enterprise.gem.co/, retrieved 09/2019.

[10] https://medicalchain.com/, retrieved 09/2019.

[11] https://encrypgen.com/the-dna-economy/, retrieved 09/2019.

[12] https://www.simplyvitalhealth.com/, retrieved 09/2019.

[13] https://hashedhealth.com/newsletter-sept-2019/, retrieved 09/2019.

[14] https://medrec.media.mit.edu/technical, retrieved 09/2019.

[15] A. Azaria, A. Ekblaw, T. Vieiraand, and A. Lippman, "MedRec: using blockchain for medical data access and permission management", in the proc. of the 2nd International Conference on Open and Big Data, IEEE, 2016, pp. 25-30.

[16] C. McFarlane, M. Beer, J. Brown, and N. Prendergast, "Patientory: a healthcare peer-to-peer EMR storage network" v1.19, https://patientory.com/, retrieved 09/2019.

[17] coinmarketcap/patientory, retrieved 09/2019.

[18] coinmarketcap/medicalchain, retrieved 09/2019.

[19] GDPR, https://eugdpr.org/, retrieved 09/2019.

[20] M. Vukolić, "Rethinking permissioned blockchains", in the proc. of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ACM, 2017.

[21] CNS, http://www.progettocns.it/, retrieved 09/2019.

[22] SPID, https://www.spid.gov.it/, retrieved 09/2019.

[23] https://hyperledger.github.io/composer/, retrieved 09/2019.

[24] https://hyperledger-fabric.readthedocs.io, retrieved 09/2019.