The Case of HyperLedger Fabric as a Blockchain Solution for Healthcare Applications

Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Rehman, M. H. U. & Kerrache, C. A.

Original citation:
Antwi, M, Adnane, A, Ahmad, F, Hussain, R, Rehman, MHU & Kerrache, CA 2021, 'The Case of HyperLedger Fabric as a Blockchain Solution for Healthcare Applications', Blockchain: Research and Applications, vol. 2, no. 1, 100012.
https://dx.doi.org/10.1016/j.bcra.2021.100012

DOI 10.1016/j.bcra.2021.100012
ESSN 2096-7209

Publisher: Elsevier

Blockchain: Research and Applications 2 (2021) 100012

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

The case of HyperLedger Fabric as a blockchain solution for healthcare applications

McSeth Antwi [a], Asma Adnane [a,*], Farhan Ahmad [b], Rasheed Hussain [c], Muhammad Habib ur Rehman [d], Chaker Abdelaziz Kerrache [e]

[a] Networks and System Research Theme, Loughborough University, Loughborough, LE11 3TT, UK
[b] Systems Security Group, Coventry University, Coventry, CV1 5FB, UK
[c] Institute of Information Security and Cyber-Physical Systems, Innopolis University, Innopolis, 420500, Russia
[d] Center for Cyber Physical Systems, Khalifa University, Abu Dhabi, 127788, United Arab Emirates
[e] Laboratoire d'Informatique et de Mathématiques, Université de Laghouat, Laghouat, 03000, Algeria

ARTICLE INFO

Keywords:
blockchain
Electronic healthcare records
Feasibility study
Healthcare
Privacy
Security
Use-case

ABSTRACT

The healthcare industry deals with highly sensitive data which must be managed in a secure way. Electronic Health Records (EHRs) hold various kinds of personal and sensitive data which contain names, addresses, social security numbers, insurance numbers, and medical history. Such personal data is valuable to the patients, healthcare service providers, medical insurance companies, and research institutions. However, the public release of this highly sensitive personal data poses serious privacy and security threats to patients and healthcare service providers. Hence, we foresee the requirement of new technologies to address the privacy and security challenges for personal data in healthcare applications. Blockchain is one of the promising solutions, aimed to provide transparency, security, and privacy using consensus-driven decentralised data management on top of peer-to-peer distributed computing systems. Therefore, to solve the mentioned problems in healthcare applications, in this paper, we investigate the use of private blockchain technologies to assess their feasibility for healthcare applications. We create testing scenarios using HyperLedger Fabric to explore different criteria and use-cases for healthcare applications. Additionally, we thoroughly evaluate the representative test case scenarios to assess the blockchain-enabled security criteria in terms of data confidentiality, privacy and access control. The experimental evaluation reveals the promising benefits of private blockchain technologies in terms of security, regulation compliance, compatibility, flexibility, and scalability.

1. Introduction

In the healthcare sector such as medical institutions and insurance companies, the infrastructure running healthcare applications and managing the related data, deals with highly critical assets. These assets include Electronic Health Records (EHRs) that hold various personal data such as names, addresses, social security numbers, medical history, etc. which must never be released to the public. However, such personal data has been the target of various cyber-attacks. To date, various medical institutions have been hacked and millions of patients' records have been stolen [1].

Several laws and regulations such as Health Insurance Portability and Accountability Act (HIPAA) [2] and the General Data Protection Regulation (GDPR) Act 2018 [3] have been put forth to provide guidelines to healthcare applications on how personal data should be managed, processed, and secured in order to avoid fraud and theft. Despite this, the healthcare industry still seems to be an easy target for hackers and this is due to the lack of technological understanding within the industry. The

* Corresponding author.
E-mail addresses: M.Antwi-15@student.lboro.ac.uk (M. Antwi), a.adnane@lboro.ac.uk (A. Adnane), ad5899@coventry.ac.uk (F. Ahmad), r.hussain@innopolis.ru (R. Hussain), muhammad.rehman@ku.ac.ae (M. Habib ur Rehman), ch.kerrache@lagh-univ.dz (C.A. Kerrache).

Production and Hosting by Elsevier on behalf of KeAi

https://doi.org/10.1016/j.bcra.2021.100012
Received 7 September 2020; Received in revised form 13 April 2021; Accepted 22 April 2021

recent attacks on the healthcare industry are evidence of data security challenges in this sector [1]. The target attacks include, but not limited to, phishing attacks and ransomware which are successful in retrieving personal data. In fact, the high success rate of ransomware attacks has shown the lack of basic security measures such as backup and system updates (e.g., Wannacry attack) [4].

Healthcare applications are very sensitive as they directly involve personal and critical data, which must be secured from unauthorized access. According to the GDPR, medical data should be held by data controllers due to the sensitive nature involved [3]. Currently, medical data is passed-on only to the concerned departments if consent is gained via the proper channel (exceptions are made for the prevention or control of pandemics and other serious threats to health). Even though legislation is improving in terms of data management; however, medical records are still at risk due to security breaches. Personal data has a high demand in the black market. According to a panel of experts at the digital health conference in 2011, a single EHR was valued at 50$ at the black market which is extremely high in comparison to $0.25 for a credit card number [5]. One incident occurred at Howard University Hospital in 2012, where the medical technician released the patients' names, addresses and medicare numbers to the black market, solely for financial gains. Other threats to the healthcare industry are caused by phishing attacks, where the hacker masquerades as an authority to induce individuals to reveal personal data. These attacks have high impacts as the revealed data can include patients' information, or employees' distinct details including social security numbers, addresses, salaries, etc. For example, the attack on Magnolia Health Corporation (MHC), where the hacker was successful to obtain substantial information about employees using a spoofed email from the CEO. Another incident is the ransomware attack on National Health Service (NHS) in 2017, where the hackers used malware to encrypt NHS files [6], this attack resulted in the cancellation of over 6900 NHS appointments.

The attacks targeting the healthcare industry not only affect patients' privacy and security, but also cause financial and reputation damages. As these attacks become more common and easy to perform, there is an urgent need for robust and reliable ways to ensure data security, confidentiality, integrity and availability to authorised users only. Various healthcare institutions have been looking into cloud-based technology and various kinds of encryption techniques. Recently, blockchain technology has been used and acclaimed as one of the promising solutions to solve the security issues in healthcare applications. Blockchain is based on a peer-to-peer distributed and decentralised computational architecture which puts emphasis on value and trust rather than the exchange of information [7,8]. The incorporation of blockchain results in compliance with the GDPR's goal of protecting data by giving control to the users and using cryptographic hashes and distributed consensus mechanisms to keep data integrity and consistency. Many researchers and developers believe that blockchain is the horizontal innovation needed to transform various industries. Even though blockchain has been heavily linked to the healthcare industry, there is a lack of research into whether the existing blockchain technologies could be used for the industry. The purpose of this study is to carry out an investigative analysis of blockchain to find out whether it is a suitable technology for the healthcare industry. To carry out the analysis, we check various scenarios to test healthcare application requirements.

The main contributions of this research paper are summarized:

(1) Identification of the healthcare applications development requirements and establishment of specific testing criteria;
(2) Design and Implementation of scenarios on HyperLedger Fabric to assess the identified requirements and criteria;
(3) Critical analysis of HyperLedger Fabric suitability for healthcare application and highlighting the needed future development.

The rest of the paper is organised as follows: Section 2 presents the discussion on the background and related works. Section 3 presents the detailed elaboration of our research methodology. Section 4 presents the design and implementation details of use case scenarios. The results are presented in Section 5 and finally the discussion and conclusion are presented in Section 6.

2. Related work

In order to secure data and prevent attacks, various solutions have been proposed to tackle such security issues in the healthcare industry. For example, Yeng et.al [9] focused on encouraging security conscious behaviour in healthcare staff and provided a comprehensive Healthcare Security Practice Analysis. The key Healthcare application architectures can be divided into two categories: 1) cloud-based solutions, and 2) blockchain-based solutions. Indeed, various cloud-based architectures have been explored within the healthcare industry, specifically for managing EHRs and patient's information [10]. Cloud computing can minimize the cost subsequently, thus, motivating to improve different healthcare services [11]. For instance, prescription expenses can be reduced by 80% while utilizing cloud-based services [12]. Due to the centralized and ubiquitous nature of cloud computing architectures, it provides a great opportunity to access data (patient or employee) anytime and anywhere. One such cloud-based system is proposed by Koufi et al., which allows physicians to access patient's medical data at any given time [13].

On the other hand, blockchain has also been leveraged to address the issues faced by the healthcare industry. For example, applications such as BitHealth and MedRec are notable blockchain-based applications to support the healthcare industry [14,15]. BitHealth uses bitcoin for storing and securing healthcare data and focuses on privacy. Bitcoin is used for payments and for insurance companies to retrieve medical history. However, it uses proof-of-work algorithm and depending on the size of the blockchain, it might be slow and energy inefficient. The other use-case, MedRed, is an EHR management system created by MIT which focuses on improving tracking of these records [16]. Patients also have some degree of control on their information and permissions are given to the patients so they can decide whether to share data with professionals or not. MedRed is based on Ethereum, it uses the same algorithm for consensus (proof-of-work) as bitcoin which is extremely costly and energy inefficient. Personal data will be stored off-chain, so users cannot determine whether the records are valid. Consequently, users' authentication is legitimate, but the data may not be accurate [17]. In Ref. [18], the authors suggested blockchain platform for efficient electronic medical record sharing while saving resources in blockchain and considered different data formats in medical records information.

Several other research projects have also suggested the use of blockchain in healthcare applications [19–25]; however, the evaluation of the proposed schemes is still not clear in the existing works.

Some studies have been conducted in order to fill this gap. We will compile their findings as well as their shortcomings to identify how the evaluation process of a blockchain application should be conducted.

There are different types of Blockchains, they could be classified into different categories: public, private, hybrid and federated/consortium.

Public Blockchains allow any user to join the blockchain (permissionless), and do not discriminate between users [26]. On the other hand, private Blockchains seem to be used more in the industry as there are more security and privacy constraints, and users need to request permission before becoming a member of the blockchain (permissioned blockchain). Members of a private blockchain can be further restricted with different access privileges. Unlike the private blockchain which is managed by a single organisation, the consortium blockchain is decentralised and is managed by multiple organisations. It is also a hybrid blockchain, it can be used by banks and food tracking, companies for example. Finally, hybrid blockchain is based on a combination of private and public Blockchains features, where users control the access to their data and a subset of the data can be put publicly available. The main advantage of a public blockchain is its autonomy. All users have similar

privileges, and no party can control the stored data, which means that users do not have to trust and rely on a third party. However, public Blockchains are extremely large and consume a large amount of energy as no user has access restrictions. On the other hand, private Blockchains tend to be smaller and flexible as only a limited number of users can access the data from the blockchain, and they have different permissions and access privileges.

In our point of view, the feasibility of blockchain itself is one of the first question that should be analysed carefully. In Ref. [27] for example, Lewis et al. focus on identifying the key challenges that could be solved by blockchain. Authors claim that blockchain is applicable to areas where trust, consensus, immutability or any mix of the 3 are the main challenges. This is a sensible place to start the evaluation process of the feasibility of blockchain but seems to be optimistic and generic. Similarly, other researchers compiled a decision tree to identify whether blockchain is necessary for a use-case [28,29]. The common drawback of these studies is that questions are often open-ended and are not specific to certain applications or not built to solve specific challenges.

The studies are not specific to any industry and lack details for any industry to adopt the findings confidently. Zhang et al. conducted an evaluation specific to the healthcare industry which will give insight into this study [30]. They developed 7-layers guidelines that a blockchain healthcare application should follow (Table 1). A major criticism of this study is that it assumes already that blockchain is applicable to the healthcare industry and fails to put any sort of weight or ranking on these guidelines [31].

In addition, researchers in Ref. [32] provided a statistical analysis of the effectiveness of HyperLedger frameworks as a tool for developers to develop their applications but was not focused on a specific application type. Similarly, Jianbi et al. [33] proposed an automated testing of blockchain-based decentralised applications. Gencer et al. developed a project called 'Miniature World' which attempts to emulate a blockchain in a virtual environment and test it in different scenarios. The testing was based on various metrics such as mining power, fairness, consensus delay and time-to-win [34]. These studies were not specific to healthcare applications and did not focus on its requirements and challenges.

T.D. Smith et al. [14] suggested a blockchain 'litmus test' where the authors surveyed blockchain applications (including MedRec) and concluded three criteria that predict success for blockchain-based data management projects, i.e., dependability, security, and trust. While Gao et al. [35] conducted a survey on the applications using blockchain (e.g., healthcare applications, IoT and cloud computing) and they assessed the primary challenges in the blockchain implementations. Although their assessment focused only on security and performance (availability and scalability) criteria, they concluded that blockchain performance is going to be one of the biggest challenges for accessing medical data, especially in emergency situations. On the other hand, Kassab et al. [36] investigated in their survey the quality requirements for blockchain-based healthcare systems and concluded that blockchain is likely to be a supplementary technology and not a replacement of the healthcare system. Blockchain can be used to handle a subset of data for specific procedures/types of data. Moreover, Bodkhe et al. [37] proposed a survey on decentralised consensus mechanisms for Cyber Physical Systems (CPS), where they considered the applicability of consensus algorithms in IoT and other areas. While analysing IoT-based applications supported by blockchain such as smart-healthcare, they concluded that there were many challenges related mainly to the conversion from centralized to decentralised system, cost, scale and associated overheads, network latency, throughput, and complex security mechanisms required to prevent double spending attack [38]. On the other hand, some experts are very sceptical about the adoption of blockchain in general. Zile et al. believe that blockchain should not be used because decentralisation is costly and not necessary; cryptocurrency is its only successful use-case for permission-less blockchain [39].

Ultimately, there are inconsistencies and gaps in the evaluation methods put forth but gives great insight into how to develop a framework for evaluation. By consolidating all these various methods and relevant information, an effective evaluation will be carried out to conclude whether blockchain should be used in the healthcare system. In this study, we aim to provide an evaluation of scenarios related to key requirements of healthcare applications in a blockchain environment. The following section will explain in detail the research methodology undertaken to achieve this aim.

Table 1
Summary of evaluation metrics [30].

	Metric	Justification
1	Entire Workflow Must be HIPAA (Health Insurance Portability and Accountability Act) Compliant	PII must be protected against a confidentiality breach
2	Blockchain Platform Should Support Turing Completeness Operations	The blockchain-based healthcare app should support Turing-complete operations, i.e., it should contain programming features capable of solving any computation problem.
3	Support for User Identification and Authentication	Two types of participants require identification/authentication in healthcare: patients and healthcare professionals
4	Support for Structural Interoperability at Minimum	Blockchain platform should enable the exchange of clinical data and interpretation of received data given the structures or formats implemented.
5	Scalability Across Large Populations of Healthcare Participants	The healthcare application may need to provide services for millions of users, it must be scalable.
6	Cost-Effectiveness	Cost estimation is important when the application provides services for large number of participants. So blockchain should be cost effective to existing solutions.
7	Support of Patient-Centred Care Model	Blockchain-based health systems should grant patients easier access/control to sharing their own medical data.

3. Research methodology

In this section, we elaborate on the blockchain evaluation approach undertaken in this study. We start by identifying key requirements of healthcare applications, and then we present the testing data in the form of scenarios which are implemented to test the identified requirements. Finally, we present the details of the tools used to develop the proposed blockchain environment. It is important to note that the purpose of this paper is to perform essential tests that we consider critical before the development of the full application (the full application is not developed in this context).

3.1. Requirements for the healthcare applications

Here, we outline the requirements of the proposed business network and identify what must be done in order to accurately replicate the healthcare applications. In order to investigate how blockchain can be leveraged, it must solve the key issues related to security, regulation compliance, scalability, and flexibility.

3.1.1. Security

The blockchain platform must ensure the basic aspects of security: availability, integrity and confidentiality, to be beneficial for the healthcare industry.

Confidentiality can be achieved by making sure that the application is on a private blockchain and has restricted access for users. This will mimic the certification required in the healthcare industry, i.e., to become a doctor, the right qualifications are needed. Similarly, in the

business network, doctors' accounts must be created by a medical institution. Further to this, the blockchain network should be permissioned to preserve data privacy. Furthermore, the participants will have different roles and privileges. Additionally, encryption must be used to make sure that data in-transit between the user and the blockchain is secure. Confidentiality is also imperative in this business network because it directly combats phishing attacks and data breaches (the most common attack on the healthcare industry) [1,4].

Integrity: Integrity means to make sure that the information is trustworthy and accurate. The blockchain must achieve this through two different ways: 1) hashing, and 2) shared distributed ledger. A strong collision-resistant and secure hashing algorithm must be used to ensure integrity. Similarly, confidentiality and access control also make sure that the data is trustworthy by limiting the number of people who can tamper with the information.

Availability: It is important that there is a reliable and easy access to information on the blockchain. By ensuring that the blockchain network is fault-tolerant, it reduces the number of failed connections to data on the blockchain. Additionally, information on a blockchain is a shared ledger, so there are various copies of the data making sure information will not disappear. The blockchain network must also run on the latest version of HyperLedger to make sure any bugs do not affect the availability of the system.

3.1.2. GDPR compliance

To test whether the healthcare industry can utilize blockchain; the business network must take steps to comply with the GDPR as much as possible. The GDPR guarantees the following rights to data subjects [3, 40]:

Transparency: Personal data should be processed lawfully and in a transparent manner.

Informed consent (collection purpose): Personal data should be collected for specified, explicit, and legitimate purposes. Data subjects require the ability to understand who and why people have access to their data.

Right to object: The data subject can object to the processing of their data, for example, for marketing or profiling purposes.

Right of access: Personal data should be securely stored and protected against unlawful processing and accidental loss, destruction, or damage.

Right to restrict access: Data subject may object to the processing of their data (e.g in case of inaccuracy).

Right of rectification: Personal data should be accurate and kept up to date. The data subjects should have the right to rectify inaccurate personal data concerning them.

Right of erasure (to be forgotten): The data subjects have the right to request the erasure of personal data concerning them.

Right of portability: The data subject has the right to obtain and reuse their data for their own purposes across different services (this assumes the data must be in a common format).

The concepts that the healthcare industry could struggle with in the development of blockchain-based applications is the Right to be forgotten. However, GDPR puts exemptions in relation to the public interest.

3.1.3. Scalability

To be used within the industry, the blockchain must be able to manage several participants with different roles and access privileges. As a result, the application must be able to deal with scenarios with multiple participants who all have different assets and data.

3.1.4. Flexibility

The blockchain must be flexible enough to deal with different data types from text to images. Medical practitioners do not only get information in the form of text, but also in the form of images such as x-rays. Failing to introduce flexibility would be unrepresentative of the industry and would exclude important pieces of information.

3.2. Testing approach

Different tests were designed to assess the essential aspects of the blockchain's network from security to fault tolerance. The tests have been derived from the requirements and dictate whether the test was a success or a failure. Each test has objectives which outline the purpose of the test; a test description outlining the methodology; an expected result and an actual result which shows the real outcome of the test. For a test to pass, the expected result must be the same as the actual result. All the tests were executed using HyperLedger Composer and HyperLedger Fabric (detailed in Section 4.2).

This work solely used manual tests to focus on intricacies and details of the blockchain. Manual tests are tests that are executed by an individual whereas automated tests are executed via scripts. Automated tests are faster and seen as more accurate but, in this project, manual tests were more appropriate. To assess specific features such as participant's access control, human intuition is imperative. Despite the increase in processing time, quick and reliable results are given for anyone to interpret. Additionally, considering the flexibility of the blockchain network, multiple scripts would need to be devised proving to be time-consuming.

HyperLedger Composer offers 3 different types of tests for blockchain applications: interactive test, automated unit tests and automated system tests. In our work, we will be using interactive tests to assess whether the scenarios could be implemented into blockchain. Interactive tests will be used to check validation, verification, permissions, and the overall performance of the blockchain network. All the tests in Table 2 will be used to evaluate the fault tolerance and efficiency of the business network.

3.3. Implementation tools and environment

3.3.1. Blockchain platform: HyperLedger Fabric

Several blockchain platforms are available as open source to allow the development of a wide range of applications. Ethereum [41], HyperLedger Fabric (IBM) [42] and Corda R3 are the most used and developed platforms in the literature nowadays [43].

A key requirement of the blockchain-based healthcare environment is to provide different levels of control to different types of users. This is only possible with permissioned frameworks like HyperLedger Fabric or Corda. Unlike Ethereum, Fabric and Corda provide more fine-grained access control, i.e., participants can be restricted to reading, creating, updating and deleting rights and thus have stronger privacy. Hence, the consensus in HyperLedger Fabric and Corda can be achieved quickly as only parties taking part in a transaction need to reach consensus. However, the Ethereum Proof of Work (PoW) consensus mechanism is processor intensive and makes it impractical in the long run [43–45].

In addition, HyperLedger Fabric offers the delete rights for users.

Table 2
Additional tests.

ID	Test description
0	Only patients can create EHRs (Electronic Health Records).
1	Participant can not view or delete an EHR that does not belong to them.
2	Only institutions can add practitioners to the business network.
3	Practitioners can only update EHRs they have been given access to.
4	Only the EHR owner can add/remove access rights from their EHR.
5	Only practitioners can record information about patient visits.
6	Only practitioners can refer patients to another practitioner.
7	Patients must be able to view when and why they have been referred.
8	Only the owner of the EHR can delete their EHR.
9	Image data (non-text) can be uploaded.
10	Only practitioners can upload images to EHRs
11	HTTPS must be used to secure the channel between the client and blockchain.

However, no data is deleted, a delete is a transaction which simply marks certain data as deleted. The number of blocks still increases with deleted transactions remaining intact. Marking transactions as deleted is the only step taken by the blockchain developers to comply with the GDPR. Even though this may not be enough to comply with various legislations, it takes bigger steps than its peers. The right to erasure, also known as the right to be forgotten, is against the blockchain principle of immutability, but it is worth investigating how blockchain-based applications could comply with GDPR in this regard.

Corda on the other hand is a platform specialized for the financial industry, where the creation of digital currencies is not intended. According to Valenta and Sandner [43], Corda's focus on financial services transactions simplified its architectural design compared to Fabric which provides an architecture to a wide range of industries. There are recent efforts to integrate Corda into the HyperLedger framework. Therefore, Corda can be considered as a complement to HyperLedger Fabric.

In this work, we used HyperLedger Fabric along with HyperLedger Composer which is a development toolset to develop business networks. One of Fabric's main capabilities is the use of identity management. This functionality allows a developer to manage user authentication and authorization. Another available functionality is related to privacy and confidentiality services. Fabric achieves this by using restricted messaging paths called private channels, which provide both confidentiality and privacy for transactions. Additionally, Fabric is atomic and its smart contracts can fail in 2 separate ways: 1) if there is an error during the execution of chain-code, the error will make the peer fail and the error is returned; 2) If a transaction is endorsed but fails later, the transaction will be rejected and logged as a failure.

Despite the benefit of Fabric cited above, there are few limitations such as the lack of built-in consistency checks, which is left for the developer to enforce in the chain-code. Consistency ensures that operations always gets the latest version of data. Further to this, Fabric's transactions are 100% durable meaning that data will always be submitted even in case of system failure. In any case, the transaction will be written to multiple nodes and as a result, it would not be lost. Finally, we used HyperLedger Composer which is a development toolset to develop business networks. Composer has a user interface for configuring, testing and deploying the business networks called Playground which is the main tool used for implementation. Playground allows developers to simulate business networks by utilizing assets (goods or services that are stored in the blockchain); participants (members of the blockchain) and transactions (methods allowing participants to interact with assets). The scenarios designed in this study are simulated in Playground (as presented in Figs. 1 and 2). Each scenario is designed through the **Define** page (Fig. 3) and tested via the **Test** page (Fig. 4).

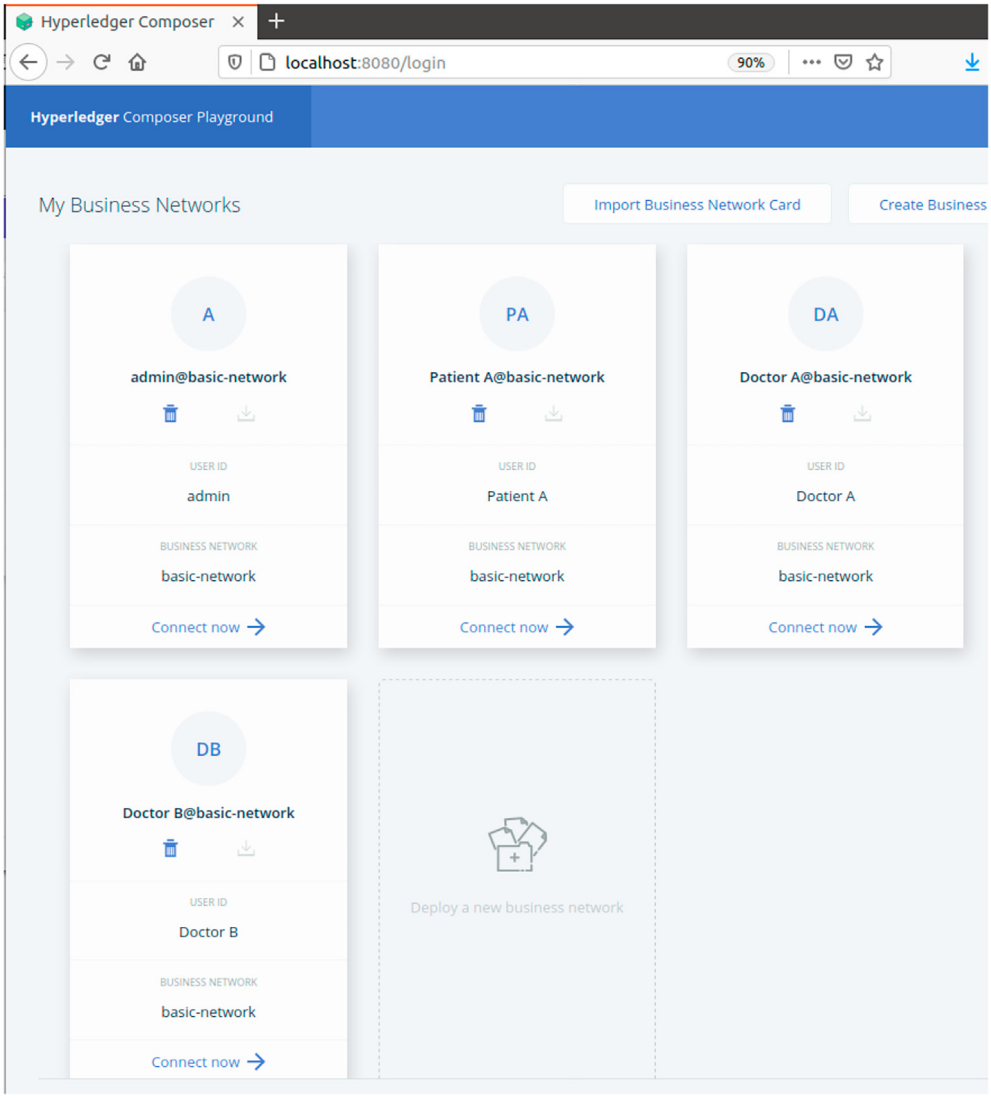

Fig. 1. Composer Playground.

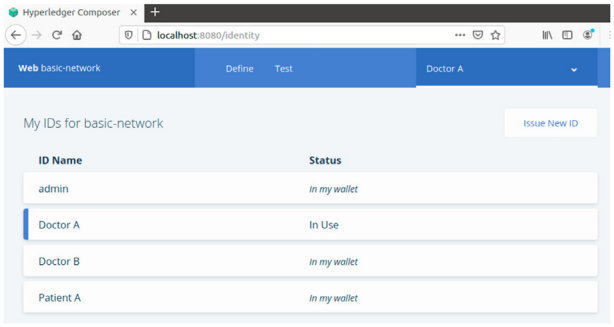

Fig. 2. Playground's users.

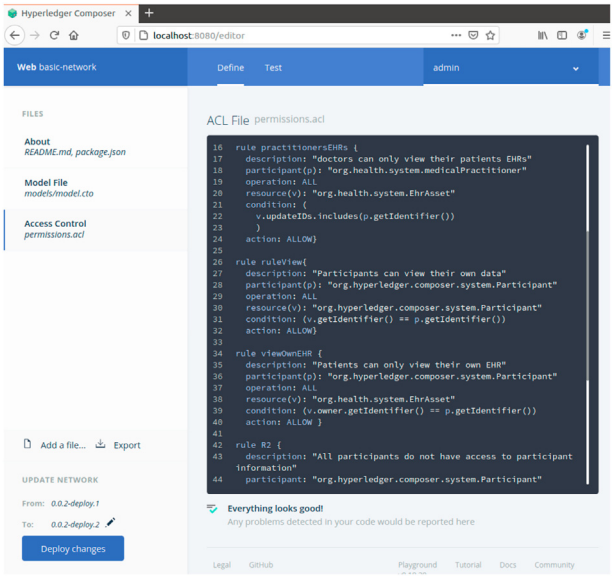

Fig. 3. Playground's define page.

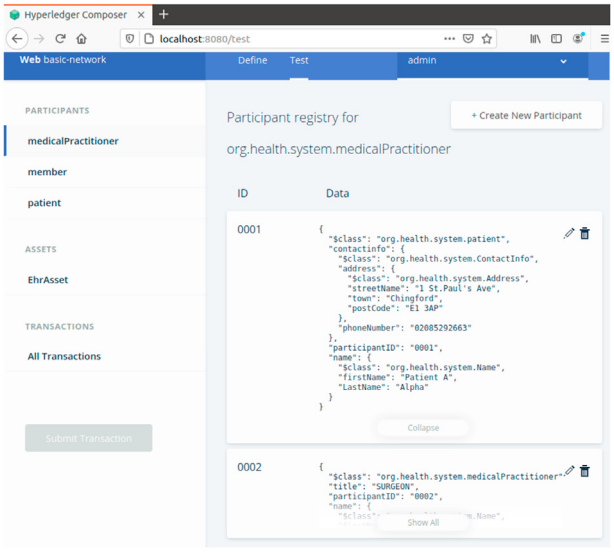

Fig. 4. Playground's test page.

3.3.2. Implementation environment

We used a 64-bit Laptop with Ubuntu OS (version 20.04.1 LTS). Blockchain can rapidly scale from small to large but using the scenarios in Section 4.2 as a blueprint, the machine specifications were enough. Larger scale blockchains would require more processing power in order to be efficient and cope with hundreds of active participants.

Before installing Fabric, the following prerequisites were required: git 2.9+; python 2.7.x; npm v5.x; Docker Engine 17.03+ and Docker-Compose 1.8+. To create the development environment various components (known as CLI tools) are required; the only compulsory component is composer-cli. However, in order to enable features such as encryption, components such as composer-rest-server are required. In order to develop and execute a business network, Composer Playground 0.19.20 and VSCode 1.51.1 were both installed. Using VSCode's marketplace the HyperLedger Composer extension was installed to ease the development. Lastly, Fabric was installed from the github official repository HyperLedger.github.io.

4. Design and implementation

The purpose of this design is to create a plan for a business network that will be developed. In this section, we highlight how different segments of the design interact with each other as well as display how scenarios will take place within the business network.

The class diagram presented in Fig. 5 illustrates how different assets and participants will interact within the blockchain network. Relationships within the systems display what transactions different participants can access as well as the multiplicity between them. As this is a blockchain, all attributes are private unless the correct permissions are given but the class diagram below is an abstract overview of how the system will work. Further to this, Fig. 5 clearly expresses any needs and dependencies classes have, giving a deeper insight into the blockchain's structure.

4.1. Users and permissions

Each participant's role and access control are charted in Table 3. These permissions and roles will mirror some of the different roles used in the healthcare sector and will illustrate how a permissioned blockchain can be utilized in different use cases.

Several transactions have been added to the developed platform in order to simulate an application and test different access rights implemented (Figs. 6 and 7), for example, a hospital account only can create practitioners' (doctors) accounts as shown in Fig. 8.

4.2. Scenario design

4.2.1. Basic scenario

This scenario tests different access control policies between a standard user and specified member of the blockchain (patients, medical institutions or medical practitioners). Specified members will be able to view data on the blockchain whereas a standard user will have no access. Further to this, this scenario confirms the use of a strong hashing function and the concept of a shared ledger. The patient and the medical practitioner should have a copy of the same transaction (Fig. 9). Participants are: User A, Patient A, and Doctor A. They will be added to the blockchain as non-admin members. The admin user will have full read and write access to the blockchain. Patient A creates an EHR and lists Doctor A as his/her doctor. Patient A and Doctor A will be able to access the EHR created by the participant whereas User A should not be able to see the EHR or have any knowledge about anyone on the blockchain.

4.2.2. Permissioned scenario

This use case tests the level of permissions utilized on Fabric regarding create, read, update, and delete operations. In this scenario, Medical institutions, patients, and practitioners will all have different permissions corresponding to Table 3. The goal of this scenario is to explore how Fabric permissions could be used to setup and manage authorisations and access control to different types of participants (Fig. 10).

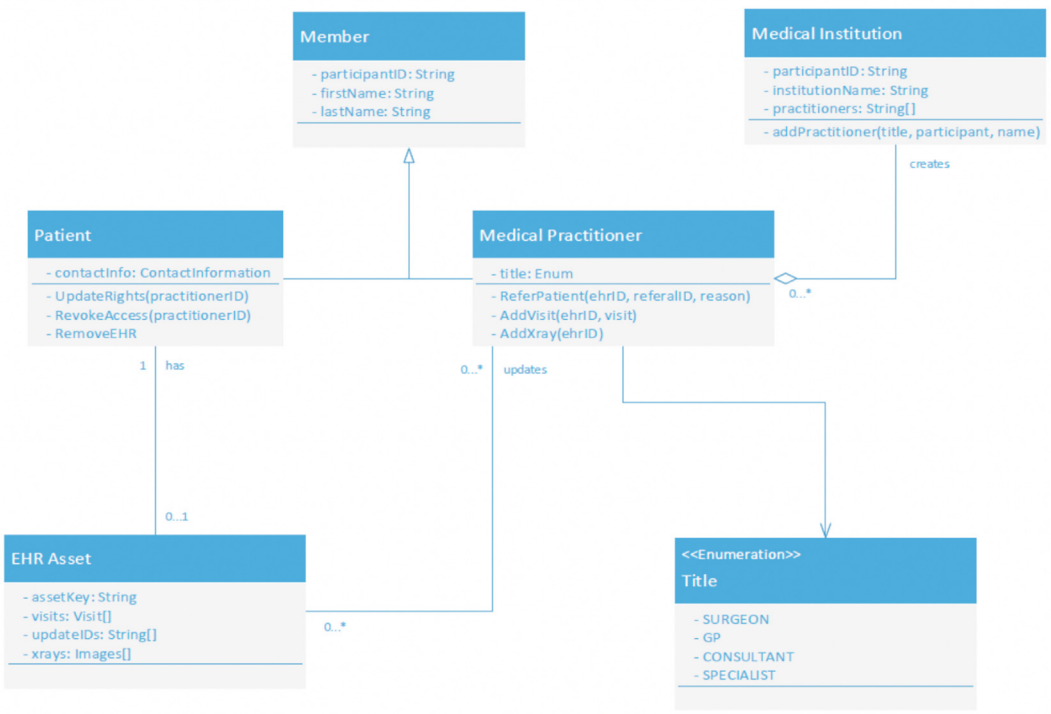

Fig. 5. Class diagram.

Table 3
Participant's permissions.

Role	Permissions
Admin	Has full access to all users and system resources.
Member	Create, delete, read and update their own participant information.
Medical institution	Create, delete, read and update their own participants information. Medical institutions such as hospitals must authorise/create doctors, pharmacists, surgeons etc as medical practitioners, it can also view their employees' participant information.
Medical practitioner	Create, delete, read and update their own participant information. Read/update permissioned EHR (electronic healthcare record): If a patient has authorised a practitioner, the latter is able to read or update the patient's EHRs. Refer to other practitioners: Practitioners can grant update rights to other practitioners on EHRs they have been authorised to update.
Patient	Create, delete, read, and update their own participant information. Grant update rights to practitioners: the patient can grant the doctor the correct permissions to update their EHR. Remove permissions from practitioners: The patient can revoke rights from a practitioner if they see fit.

4.2.3. *Purging scenario*

To be GDPR/HIPAA compliant, patients must have complete control over their EHRs, this includes both giving patients the ability to remove read rights from reading the EHR and deleting the EHR. The GDPR states the user must have the right to be forgotten. Consequently, this use case tests the removal of patient data (Fig. 11). Patient **A**'s GP is currently GP **A**, patient **A** moves and as a result, GP refers patient **A** to GP **B**. To minimize the number of people who have access to his/her EHR, Patient **A** revokes access from GP **A**. Additionally, patient **B** has heard of a recent security breach to EHRs and as a countermeasure patient **B** deletes his/her EHR.

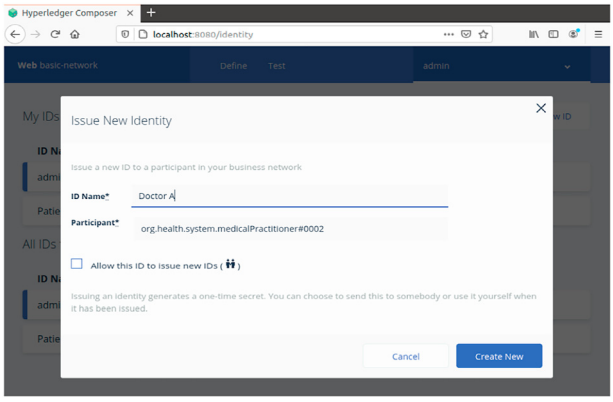

Fig. 6. Create new blockchain user.

4.2.4. *Data type scenario*

This use case tests how Fabric interacts with different kinds of data. Within this scenario, the blockchain will have to cope with images and text to mimic the data used within the healthcare industry, such as X-Rays and their annotations (Fig. 12). Patient **A** goes for an x-ray to specialist **A** and subsequently gives specialist **A** rights to update his/her EHR. Unlike purging data scenario, a reason explaining why specialist **A** was given rights will be included within the transaction. This ensures patient **A** knows why participants have access to his/her data as well as who has access. Later, specialist **A** uploads an image to an application which then converts the image to base 64. The image in base 64 is then uploaded to Fabric and stored for future referral and transformations.

4.2.5. *Encryption scenario*

This use case tests what cryptographic capabilities are available on Fabric. For example, to ensure that connection to the blockchain is secure and protected from man-in-the-middle attacks, a level of security must be available (Fig. 13).

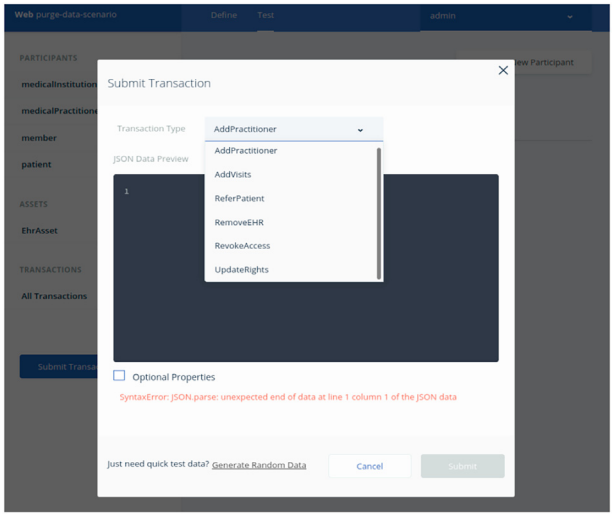

Fig. 7. List of transactions.

5. Experimental results

In this section, we discuss the results from the implemented scenarios in the blockchain environment.

5.1. Security

Throughout each scenario, validation has been made to increase the fault-tolerance of the developed blockchain. Even though Fabric is described as fault-tolerant; it does not enforce any fault-tolerance within chain-code leaving it up to the developer. The Basic Scenario used access control to restrict resource utilization to named roles (patients, medical practitioners, and medical institutions). This achieves a superficial level of confidentiality by keeping personal data private to blockchain participants. Further to this, Basic Scenario showcases 2 key concepts of a blockchain: shared ledger and hashing which together achieve an acceptable level of integrity. SHA-2 was used to hash each transaction ensuring users that the transaction is accurate. There is no known breach to SHA-2 making it near impossible for a hacker to replace or create a transaction that fits to the blockchain. The concept of a shared ledger ensures that data within the system is accurate and unaltered because all peers of the blockchain have their own copy. Basic Scenario alone shows 2 key concepts which are enough to achieve integrity but leaves much to be desired in regards to confidentiality. Permissioned Scenario scaffolds from Basic Scenario and implements various access controls providing confidentiality between different participants on the blockchain. By granting different permissions to different roles within the blockchain, the number of users who have access to patients' personal data is significantly reduced, which will reduce the risk of data breach. Fig. 14 shows the doctor has no access to patients or their EHRs, when patients update their EHR access rights and give the doctor access (Figs. 15 and 16), the doctor can view the EHR and update it after each visit (Fig. 17). Note that in each scenario we tested the user permissions, for example, patients can control who has access to their EHR but they cannot add visit details to their EHR (Fig. 18).

With Encryption Scenario, confidentiality is fully achieved by protecting data outside of the blockchain. Basic Scenario and permissioned scenario achieved confidentiality on the blockchain but fail to protect any in-transit data. This scenario creates a bespoke REST API to encrypt and protect data being transmitted between the client and the blockchain. Elliptic-Curve Diffie Hellman (ECDH) is used as the key exchange with the public-private key pair, and AES128 is used as the symmetric encryption method.

5.2. Regulation compliance

A part of this work was to assess whether HyperLedger could comply with the GDPR [40] (rules detailed in Section 3.1.2) which are tested in Basic scenario and Permissioned scenario. Fig. 19 shows that patients can view their data, while Fig. 20 shows the ability for a patient to restrict/remove data access to practitioner (Fig. 21 shows the list of successful transactions). In addition, in the permissioned scenario, patients can control how long practitioners have access to their EHR (Right of erasure).

Although blockchain does not allow removing data, or controlling how the shared data will be processed, the introduction of different access control rules grants patients the ability to control who has access to their EHRs, which comply with the GDPR right of access and right to

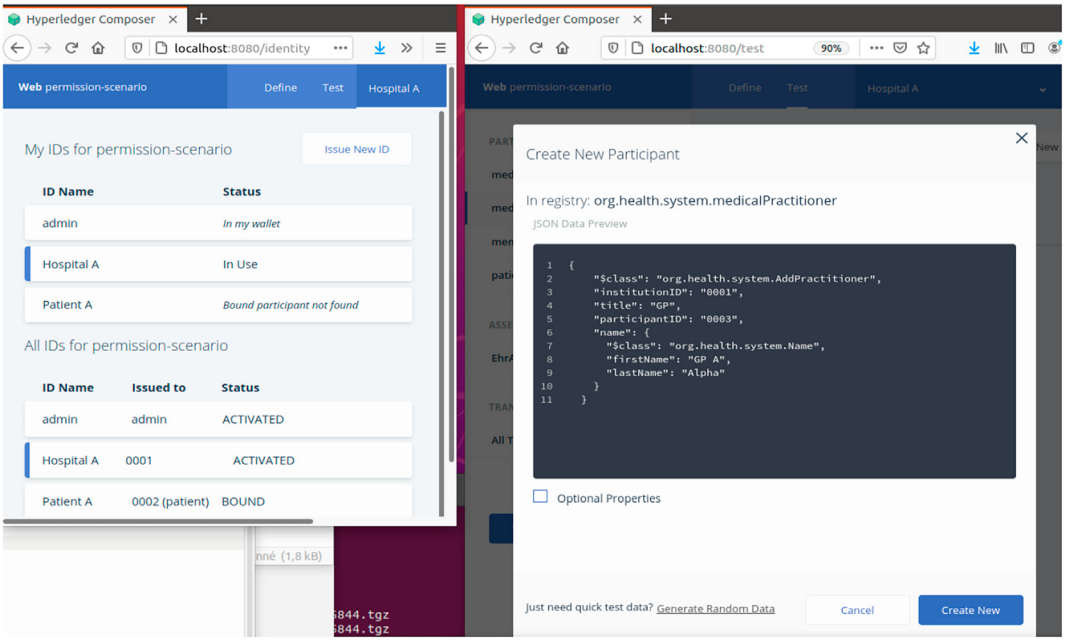

Fig. 8. Hospital account only can create a practitioner.

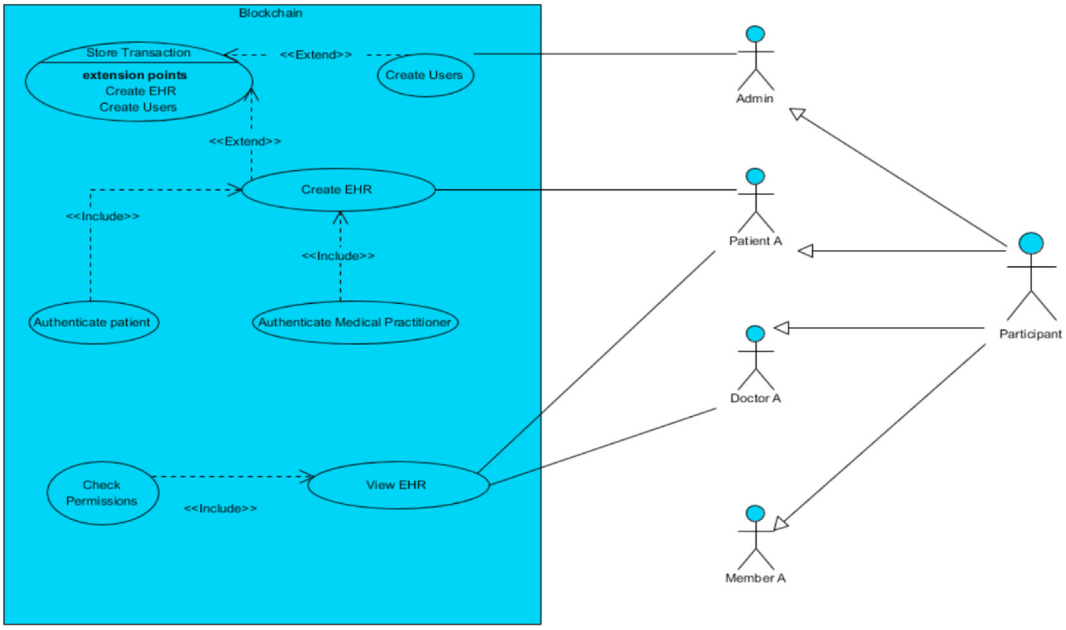

Fig. 9. Basic scenario — UML use case diagram.

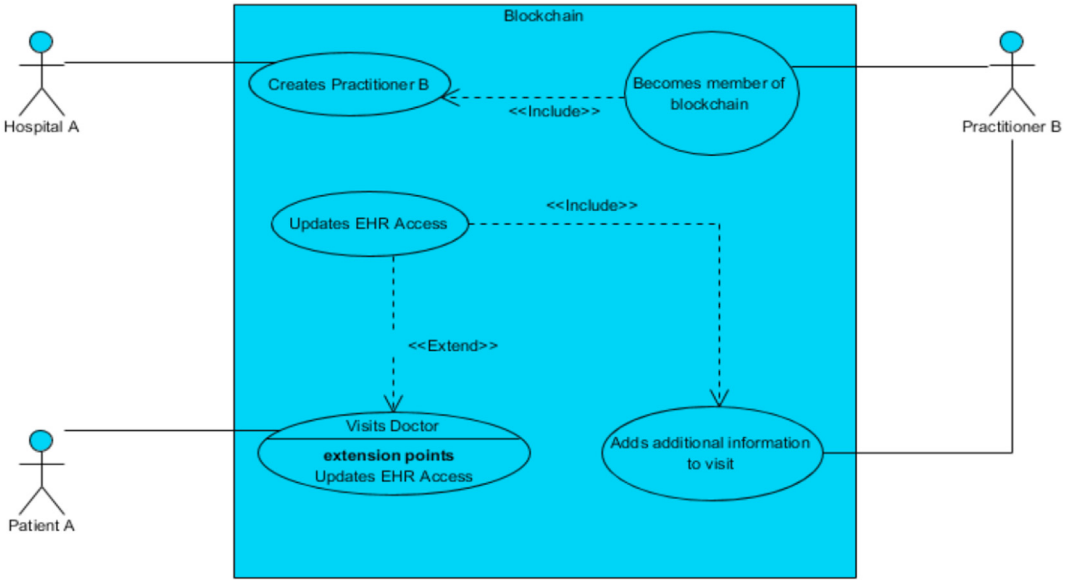

Fig. 10. Permissioned scenario - UML use case diagram.

restrict access. If the patients deny access to their EHR, they can at least ensure that no practitioner will have access to their data which could be considered as data removal, as the data is only available to the patient.

Unlike HIPAA, the GDPR states individuals have the right to erasure which Purging Data Scenario examines [46]. Composer allows participants to delete their own data as shown in Fig. 23) (which is not allowed for other users — Fig. 22). Superficially, it seems that HyperLedger complies with the GDPR and can delete data. However, Composer is simply a higher-level tool-set which runs on top of Fabric. Transactions are simply marked as deleted and appear that way in Composer but at the Fabric level, the transaction remains unchanged. If Fabric is the network level; Composer would be the application layer. To cooperate with regulations, some blockchain application designers suggested HyperLedger-built applications must not store any sensitive data and it is recommended that all personal data should be stored in an off-chain database [47–49]. However, as we explained above, patients have access restriction control over their data, deletion could be replaced by denying any access to their EHR data by any other user.

HIPAA and the GDPR enforce consent through authorization and right to be informed respectively [46]. Though the GDPR takes it a step further and requires individuals to be notified if there are any changes regarding access or purpose. Data type scenario demonstrates this right by recording the reason for referral in each transaction. Patients can see why specific medical practitioners access their EHR by checking their transaction list.

Although in this paper we focused on GDPR as a data privacy regulation, there are many others around the world such as the Australia's Privacy Act 1988, Data Privacy Act 2018, California Consumer Privacy Act (CCPA, January 1, 2020), and the Nevada privacy law (October 1, 2019). They are different but they all aim to achieve many of the same things, such as the right to erasure and the right to access data.

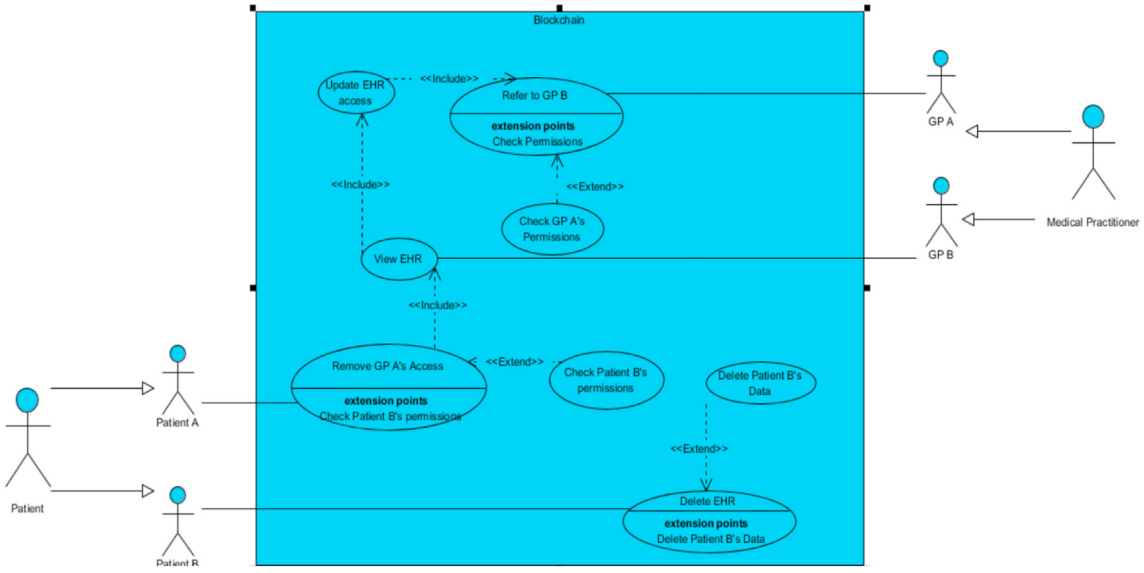

Fig. 11. Purging scenario — UML use case diagram.

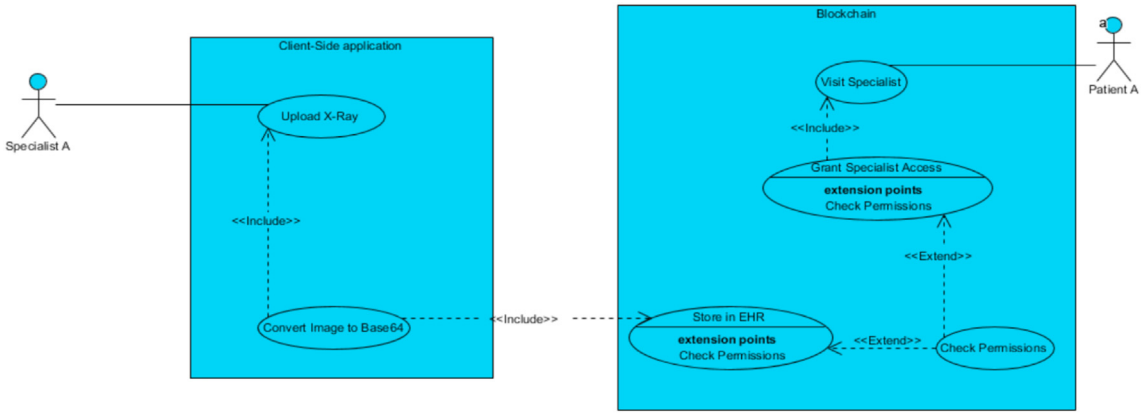

Fig. 12. Data type scenario — UML use case diagram.

5.3. HyperLedger test analysis - scalability and flexibility

Our test results revealed that Fabric is not very flexible and expects certain functionalities to be carried out on the application side. Fabric is designed to deal with only text-based data, there is no innate support for images or audio. Data type scenario shows that Fabric can cope with images but only with some outside interference. Within the scenario, a theoretical application on top of the blockchain converts the image to base64 which can then be stored on the blockchain. Fabric does not deal with data in any unique way and is unaffected by base64. Alternatively, an image could be stored in a database and the reference could be stored within Fabric but that adds another layer of complexity and security risks. Ultimately, storing images in base64 is not a major issue for healthcare. Base64 does not reduce the quality that physicians may need to see but simply changes the way the data is represented whilst compressing data. Furthermore, Fabric does not require the capability to store images or audio directly as they are not being treated any differently within the blockchain (Fig. 25 shows the image details in the EHR after the transaction Fig. 24 was executed by the doctor).

Moreover, Fabric fails to solve the issue of limited computational resources. As the system scales, so does the number of computation resources needed on each peer. For blockchain to be adopted by the healthcare industry, energy consumption and computational resources will have to be evaluated. It has become standard for blockchain platforms to offer some sort of encryption, but Fabric allows developers to use what encryption methods they see fit. This is extremely beneficial within the industry as it allows hospitals to protect their data with the latest forms of encryption rather than waiting for HyperLedger to release an update. Despite the flexible encryption, Fabric offers no chain-code level encryption. It is obvious that Fabric expects all sensitive data to be stored off-chain which is why it only offers encryption to in-transit data.[1] This feature of Fabric seems to be an answer to all the criticisms blockchain has been getting regarding data immutability. If data is stored off-chain, then the data immutability of a blockchain becomes less of a significant problem.

5.4. Additional test results

Adopting blockchain within the industry would drastically increase transparency and integrity. It would be extremely difficult to impersonate a patient within the developed business network, further limiting the superficial cyber-attacks within the industry. Additionally, the encryption capabilities of TLS could potentially protect the healthcare industry from more complex cyber-attacks. As the industry continues to adopt more cloud applications, blockchain will become more attractive.

[1] https://sxi.io/offchain-storage-in-hyperledger-fabric/.

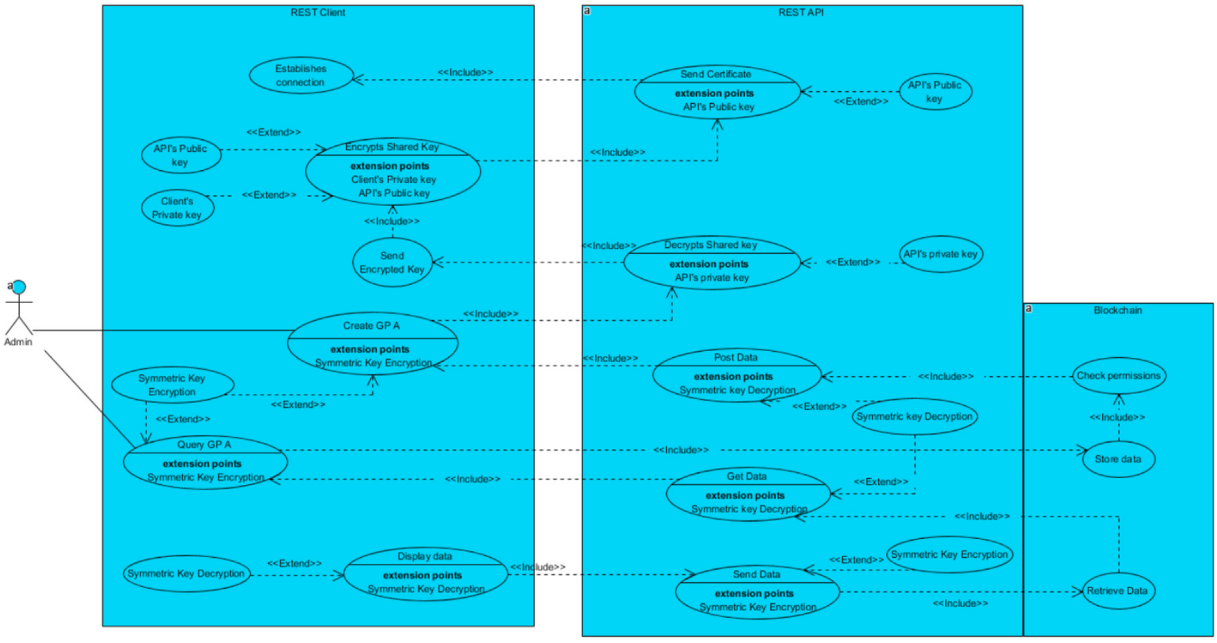

Fig. 13. Encryption scenario — UML use case diagram.

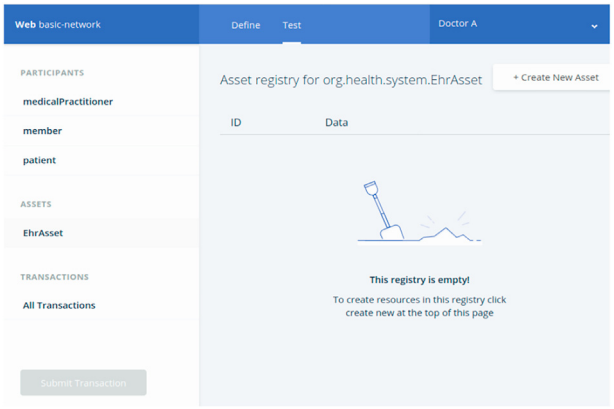

Fig. 14. Doctor has no access to electronic healthcare records.

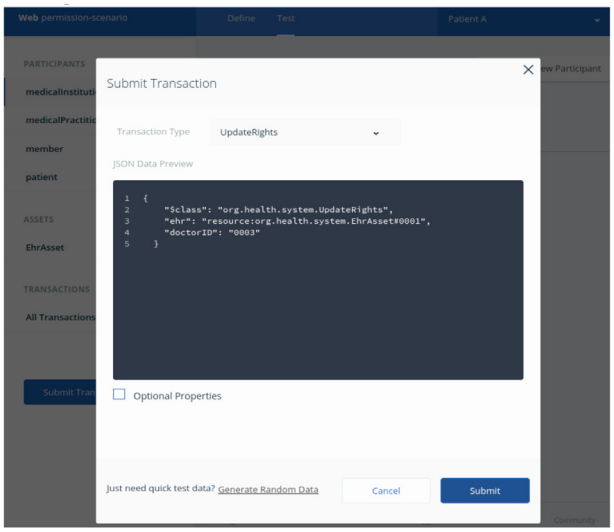

Fig. 15. Patient updates access to his electronic healthcare record.

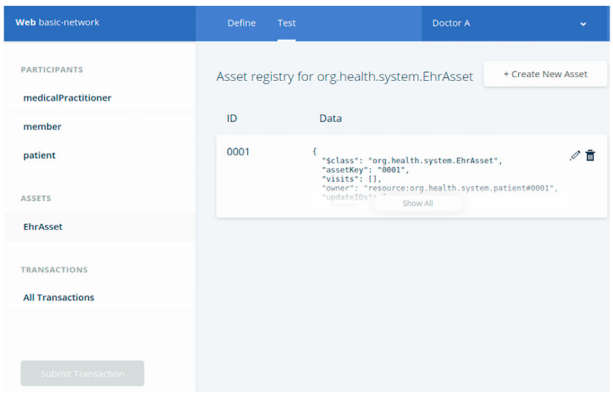

Fig. 16. Doctor has now access to electronic healthcare record.

The DPA 2018, HIPAA, and GDPR are set out to give more control to patients, but cloud solutions lack control as the vendor is responsible for infrastructure security and management. The permissioned blockchain proposed in Permissioned Scenario grants patients control with transparency which no other platform would be able to offer. Ninety-four percent of the additional test shown in Table 2 passed, showing multiple aspects of the business network's fault-tolerance. The blockchain was able to throw multiple custom-built errors to ensure the accuracy and reliability of the data. Even though the business network was not designed for commercial use, a rudimentary level of fault tolerance was needed to showcase Fabric's capabilities.

Test 10 failed when we tried referring one patient to a non-assigned id. The test failed due to the **incompatibility** of the permissions designed (Section 4.1). The business network was permissioned in a way where practitioners had no knowledge of patients unless a relationship was formed. Consequently, throwing an error would alert medical professionals to what IDs exist and compromise confidentiality. Confidentiality prioritised fault-tolerance as a requirement and was kept within the business network. This test result shows us that not all access control mechanism should be implemented on the blockchain but should be used in conjunction with client-side applications' access control. Ultimately, there seems to be a minuscule trade-off between fault-tolerance and

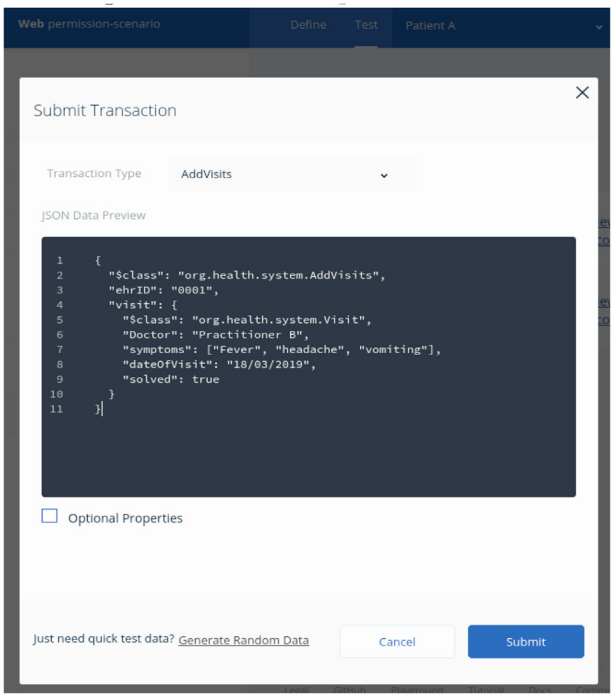

Fig. 17. Doctor updates the electronic healthcare record.

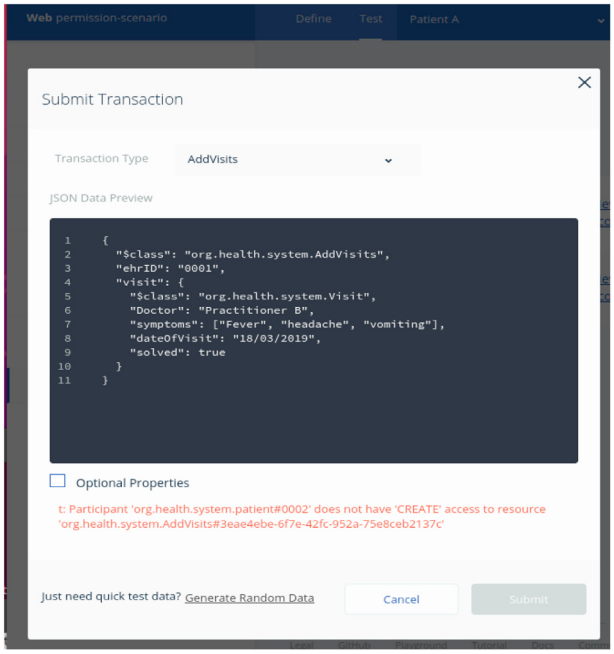

Fig. 18. Patients cannot add visits.

confidentiality.

5.5. Summary of test results

We have assessed different elements and capabilities in the previous tests through different scenarios. Our goal is not to create a complete application but to test the different blockchain capabilities before the application design.

It was demonstrated that Fabric is a shared ledger with different users permissions, but to further increase confidentiality, transactions are hidden at the composer level if the transaction does not affect the participant. In addition, as patients can control access to their EHR (Give access to a practitioner, define how long the access can last for and deny the access), we can assume the Fabric complies with the key GDPR requirements: right of access, right to restrict access and the right of erasure (personal data should not be kept longer than someone needs it).

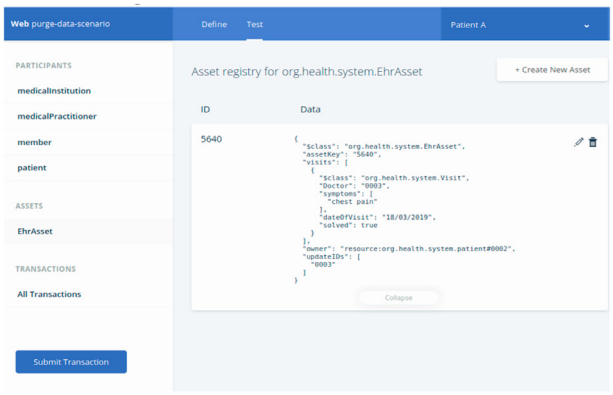

Fig. 19. Patient view electronic healthcare records.

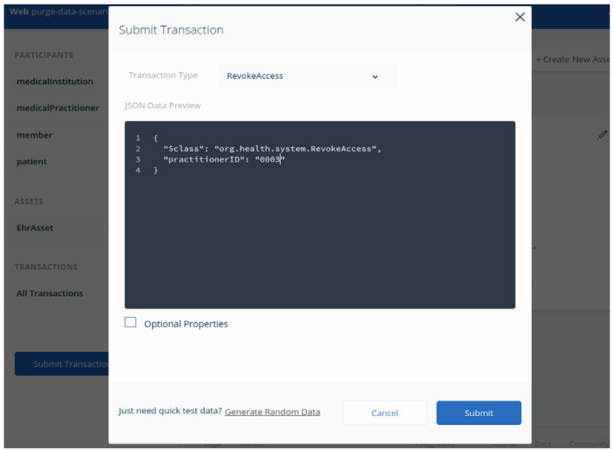

Fig. 20. Patient removing Practitioner (#0003) from their electronic healthcare record.

Finally, we have tested the different data types that could be stored in the HyperLedger Fabric which does not accept any other form of data but text, it is easy to implement an application layer that will convert any data in to text (converting Base64 does not reduce the quality of the image). Fabric's reluctance to support non-text-based data reinforces the notion that Fabric wants data to be stored in an external database, which has been supported by other researchers [47–49], although we believe that this will add another layer of complexity and security risks. Overall, Fabric allows different ways and flexibility in terms of application design and development. For example, we have seen that the developers can decide what encryption methods to use. However, all those points must be acknowledged and taken into account in the development of the application layer or the client side application.

The testing data is in the form of several files (configuration and scenarios), and is made available in a public github repository: https://github.com/asmaadnane/Blockchain-healthcare.

6. Discussion and conclusion

Throughout this work, multiple problems have been identified within the healthcare sector where blockchain is proposed as a solution to secure EHR. The healthcare industry has been identified as an 'easy' target for cyber-attacks but does blockchain reduce the security risks? As

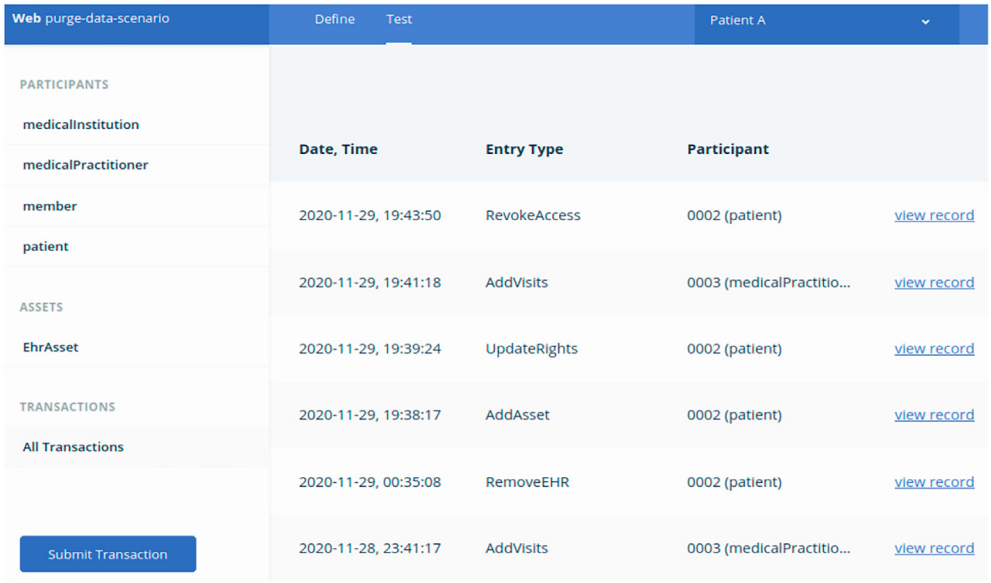

Fig. 21. Patient transactions list.

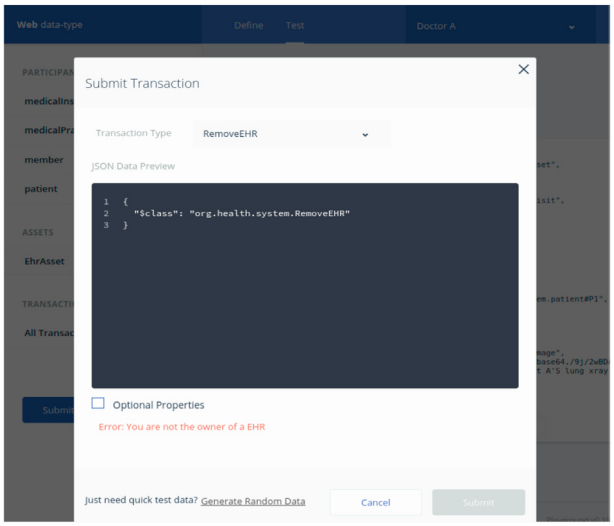

Fig. 22. Doctor cannot delete patient's electronic healthcare record.

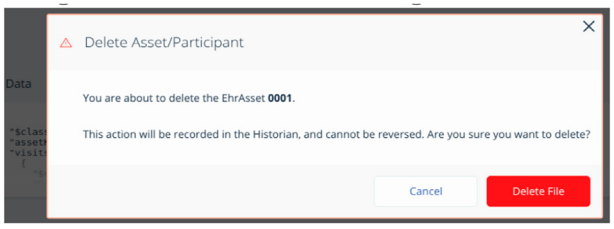

Fig. 23. Patient deleting their electronic healthcare record.

shown in the results, blockchain offers authenticity making it near impervious to impersonation attacks. Further to this, the encryption capabilities displayed by blockchain make it safe from man-in-the-middle attacks. Most importantly, the access control of blockchain restricts the number of people who can view EHR data. As a result, data breaches are less likely to occur.

Does this mean that blockchain solves healthcare security threats? If sensitive data is stored on the blockchain, the security benefits solve both

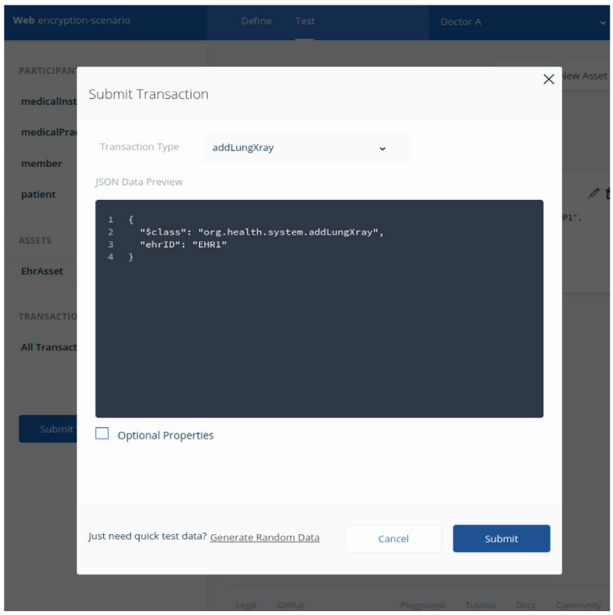

Fig. 24. Doctor adding X-ray.

the high and low-level cyberattacks. However, it has been shown that Fabric developers are suggesting data storage. A blockchain in this form only protects reference data; reducing blockchain to a lookup table which does not provide any security on actual personal data. Sensitive data must be stored on the blockchain to benefit the healthcare industry resulting in applications taking more responsibility. The application must convert all data to text; provide script-level encryption and a degree of access control to accommodate for blockchain's weaknesses.

Unlike blockchain, the cloud offers ubiquitous resources and is optimised for IoT. Despite this, blockchain still provides a better platform for healthcare as security is a necessity rather than an ideal function. It is essential that the scale of any blockchain application must be managed; blockchain, in its current iteration, exponentially requires more resources as the size increases. Even though, many of the security features implemented are not exclusive to blockchain. Security is the responsibility of the vendor, allowing for less flexibility within the

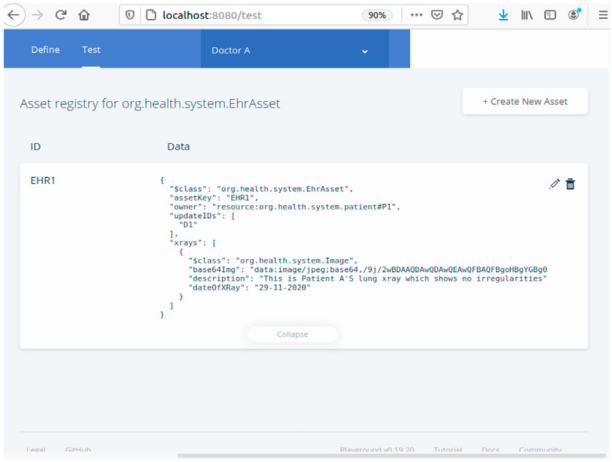

Fig. 25. Image stored in an electronic healthcare record.

industry. Blockchain allows developers to easily design their security functions such as changing the encryption algorithms, which is not the case for cloud computing.

If blockchain technology was to be developed for healthcare, there is a trade-off between transparency and confidentiality that the industry should be aware of. Blockchain is intended to increase trust by sharing all data. Yet, access control offers limits to data sharing and achieves a level of confidentiality. Any platform implementation must ensure that the access control is restricted only to identifiable data and still allows a level of transparency on the blockchain for other data types/categories.

Blockchain is not often considered when discussing regulation compliances but in this paper, we highlighted various areas where Fabric platform complies with the regulations. The biggest issue hindering GDPR compliance is the inability to remove data; however, we believe that this might not be an issue in the case of healthcare applications where EHRs do not need to be deleted. Instead, blockchain platforms, such as Fabric, give a complete autonomy to the patients, so that they have full control over their EHR and they can decide who can access their health record and for what purpose.

As countries become more aware of the energy consumption of existing blockchains, the chance of legislation changing to accommodate the emergence of blockchain is extremely slim. The trade-off between computational overhead and security cannot be made if blockchain stores sensitive data. Ultimately, Fabric provides security benefits to the healthcare industry and would reduce the number of cyberattacks. Yet other blockchain platforms in their current iteration are not suitable for healthcare. Although certain research suggested using a blockchain with a relational database to store the data, this could create new risks to personal/critical data security and privacy directly.

Blockchain presents significant security benefits but it suffers from an even larger trade-off in the form of overheads and regulation compliance. Legislation takes a significant amount of time to adapt to technology; the data protection act stayed the same between 1997 when it was first proposed to 2018 when it was updated. Alternative technologies, such as cloud computing can completely comply with the GDPR as well as offering a surplus of resources cheaply. Whereas the implementation of certain blockchain applications struggles to comply with the GDPR and requires a large number of resources as the system scales. However, blockchain is only in its 2nd generation with bitcoin being the first generation. As more time and finance are invested into blockchain, it may become viable to not only healthcare but multiple different industries. According to the recent Hyperledge announcement,[2] Hyperledge seems to have a stable future. Indeed, there are 23 Hyperledger Certified Service Providers (HCSPs) based in markets around the world, including Canada, China, India, Japan, Republic of Korea, Switzerland and the USA. Further, several companies on the recent Forbes Blockchain 50 list named at least one Hyperledger technology as part of their solution platform.

Finally, our work is the first to study preliminary healthcare applications constraints and how they could be implemented in blockchain platforms such as Fabric. The focus was on the healthcare applications characteristics rather than the large set of options and capabilities offered by any blockchain platform. This **evaluation** study contributed to defining the key criteria for the implementation of secure blockchain-based healthcare applications. Although we have not evaluated the performance parameters and the tests have been made in Fabric only, similar evaluation can be made on other platforms, or other criteria such as the performance could be evaluated. It is important to point out that the evaluation should be based on the applications constraints and needs, as well as which blockchain platform will be the best to answer those constraints and needs while ensuring good performances and data security.

For future work, we plan to use HyperLedger Explorer tool to help explore consensus, peers, blocks, and energy consumption. Using explorer in conjunction with a developed blockchain would only provide further details into how blockchain could be utilized within the healthcare industry. Finally, blockchain performance will be evaluated under a different set of Healthcare applications' requirements.

[2] https://www.hyperledger.org/announcements/2021/02/25/hyperledger-unveils-plans-for-2021-global-forum.

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.

References

[1] S. Argaw, N. Bempong, B. Eshaya-Chauvin, A. Flahault, The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review, in: BMC Medical Informatics and Decision Making, vol. 19, 2019.
[2] Health insurance portability and accountability act of 1996, 104th Congress Public Law 104191.
[3] Council of European Union, Reform of Eu Data Protection Rules, European Commission, 2018.
[4] A. Le-Bris, W. El-Asri, State of Cybersecurity & Cyber Threats in Healthcare Organizations, 2017.
[5] L. Adefala, Healthcare experiences twice the number of cyber attacks as other industries, Fortinet (March 2018). URL www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.
[6] D. Gayle, A. Topping, I. Sample, S. Marsh, V. Dodd, NHS Seeks to Recover from Global Cyber-Attack as Security Concerns Resurface, Guardian News and Media, 2017.
[7] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: a comprehensive survey, IEEE Communications Surveys Tutorials 21 (2) (2019) 1676–1717.
[8] F. Ahmad, Z. Ahmad, C.A. Kerrache, F. Kurugollu, A. Adnane, E. Barka, Blockchain in internet-of-things: architecture, applications and research directions, in: International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1–6.
[9] P.K. Yeng, B. Yang, E.A. Snekkenes, Framework for healthcare security practice analysis, modeling and incentivization, in: 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 3242–3251.
[10] E. Markakis, Y. Nikoloudakis, E. Pallis, M. Manso, Security assessment as a service cross-layered system for the adoption of digital, personalised and trusted healthcare, in: IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 91–94.
[11] H. Abrar, S.J. Hussain, J. Chaudhry, K. Saleem, M.A. Orgun, J. Al-Muhtadi, C. Valli, Risk analysis of cloud sourcing in healthcare and public health industry, IEEE Access 6 (2018) 19140–19150.
[12] O. Ali, A. Shrestha, J. Soar, S.F. Wamba, Cloud computing-enabled healthcare opportunities, issues, and applications: a systematic review, Int. J. Inf. Manag. 43 (2018) 146–158, https://doi.org/10.1016/j.ijinfomgt.2018.07.009.
[13] V. Koufi, F. Malamateniou, G. Vassilacopoulos, Ubiquitous access to cloud emergency medical services, in: 10th IEEE International Conference on Information Technology and Applications in Biomedicine, 2010, pp. 1–4.
[14] T.D. Smith, The blockchain litmus test, in: IEEE International Conference on Big Data (Big Data), 2017, pp. 2299–2308.

[15] J. Cordwell, Blockchain in healthcare: from theory to reality, in: DXC.Technology, 2015 available online: https://blogs.dxc.technology/2015/10/30/blockchain-in-healthcare-from-theory-to-reality/ (Accessed: 9th January, 2020).
[16] N. Nchinda, A. Cameron, K. Retzepi, A. Lippman, Medrec: a network for personal information distribution, in: 2019 International Conference on Computing, Networking and Communications (ICNC), 2019, pp. 637–641.
[17] A.R. Lee, M.G. Kim, I.K. Kim, Sharechain: healthcare data sharing framework using blockchain-registry and fhir, in: 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2019.
[18] S. Wu, J. Du, Electronic medical record security sharing model based on blockchain, in: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, ICCSP '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 13–17, https://doi.org/10.1145/3309074.3309079.
[19] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, F. Wang, Blockchain-powered parallel healthcare systems based on the acp approach, IEEE Transactions on Computational Social Systems 5 (4) (2018) 942–950.
[20] J. Qiu, X. Liang, S. Shetty, D. Bowden, Towards secure and smart healthcare in smart cities using blockchain, in: 2018 IEEE International Smart Cities Conference (ISC2), 2018, pp. 1–4.
[21] K.M. Hossein, M.E. Esmaeili, T. Dargahi, A. khonsari, Blockchain-based privacy-preserving healthcare architecture, in: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019, pp. 1–4.
[22] T.K. Dasaklis, F. Casino, C. Patsakis, Blockchain meets smart health: towards next generation healthcare services, in: 9th International Conference on Information, Intelligence, Systems and Applications, 2018, pp. 1–8.
[23] P. Ndayizigamiye, S. Dube, Potential adoption of blockchain technology to enhance transparency and accountability in the public healthcare system in South Africa, in: 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019, pp. 1–5.
[24] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, B. Sadoun, Habits: blockchain-based telesurgery framework for healthcare 4.0, in: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), 2019, pp. 1–5.
[25] J. Hathaliya, P. Sharma, S. Tanwar, R. Gupta, Blockchain-based remote patient monitoring in healthcare 4.0, in: 2019 IEEE 9th International Conference on Advanced Computing (IACC), 2019, pp. 87–91.
[26] D. Appelbaum, S.S. Smith, Blockchain Basics and Hands-On Guidance: Taking the Next Step toward Implementation and Adoption, CPA, 2018.
[27] R. Lewis, 30 things you can do with a blockchain, [online] https://medium.com/@rhian_is/30-things-you-can-do-with-a-blockchain-85ca9f094a18 [Accessed July 2020].
[28] S.K. Lo, X. Xu, Y.K. Chiam, Q. Lu, Evaluating suitability of applying blockchain, in: 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), 2017, pp. 158–161.
[29] M.E. Peck, Blockchain world - do you need a blockchain? This chart will tell you if the technology can solve your problem, IEEE Spectrum 54 (10) (2017) 38–60, https://doi.org/10.1109/MSPEC.2017.8048838.
[30] P. Zhang, M.A. Walker, J. White, D.C. Schmidt, G. Lenz, Metrics for assessing blockchain-based healthcare decentralized apps, in: 2017 IEEE 19th International Conference on E-Health Networking, Applications and Services (Healthcom), 2017, pp. 1–4.
[31] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: a data processing view of blockchain systems, IEEE Trans. Knowl. Data Eng. 30 (7) (2018) 1366–1385.
[32] T.Q. Ban, B.N. Anh, N.T. Son, T. Van Dinh, Survey of hyperledger blockchain frameworks: case study in fpt university's cryptocurrency wallets, in: Proceedings of the 2019 8th International Conference on Software and Computer Applications, ICSCA '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 472–480.
[33] J. Gao, H. Liu, Y. Li, C. Liu, Z. Yang, Q. Li, Z. Guan, Z. Chen, Towards automated testing of blockchain-based decentralized applications, in: Proceedings of the 27th International Conference on Program Comprehension, ICPC '19, IEEE Press, 2019, pp. 294–299, https://doi.org/10.1109/ICPC.2019.00048, 10.1109/ICPC.2019.00048.
[34] A.E. Gencer, E.G. Sirer, Miniature world: measuring and evaluating blockchains [July 2020], https://hackingdistributed.com/2017/02/10/miniature-world/, 2017.
[35] W. Gao, W.G. Hatcher, W. Yu, A survey of blockchain: techniques, applications, and challenges, in: 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1–11.
[36] M. Kassab, J. DeFranco, T. Malas, G. Destefanis, V.V. Graciano Neto, Investigating quality requirements for blockchain-based healthcare systems, in: 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2019, pp. 52–55.
[37] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P.K. Singh, W. Hong, A survey on decentralized consensus mechanisms for cyber physical systems, IEEE Access 8 (2020) 54371–54401.
[38] C. Natoli, V. Gramoli, The blockchain anomaly, in: 2016 IEEE 15th International Symposium on Network Computing and Applications, NCA), 2016, pp. 310–317.
[39] K. Zile, R. Strazdina, Blockchain use cases and their feasibility, Appl. Comput. Syst. 23 (1) (2018) 12–20.
[40] P. Voigt, A.v. d. Bussche, The EU General Data Protection Regulation: A Practical Guide, Springer Publishing Company, Incorporated, 2017.
[41] V. Buterin, Ethereum Whitepaper, 2013.
[42] C. Cachin, Architecture of the Hyperledger Blockchain Fabric, 2020.
[43] M. Valenta, P. Sandner, Comparison of ethereum, hyperledger fabric and corda, in: F. S. of Finance & Management gGmbH (Ed.), Frankfurt School Blockchain Center www.fs-blockchain.de.
[44] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of blockchain-based systems for architecture design, in: IEEE Conference on Software Architecture, 2017, pp. 243–252.
[45] P. Sajana, M. Sindhu, M. Sethumadhavan, On blockchain applications: hyperledger fabric and ethereum, Int. J. Pure Appl. Math. 118 (18) (2018) 2965–2970.
[46] S.A. Tovino, The HIPAA privacy rule and the EU GDPR: illustrative comparisons, Seton Hall Law Rev. 47 4 (2017) 973–993.
[47] Q. Lu, X. Xu, Adaptable blockchain-based systems: a case study for product traceability, IEEE Software 34 (6) (2017) 21–27.
[48] H.T. Vo, A. Kundu, M.K. Mohania, Research directions in blockchain data management and analytics, Proc. EDBT (2018) 445–448.
[49] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, B. Gipp, On-chain vs. off-chain storage for supply- and blockchain integration, Inf. Technol. 60 (5–6).