UNIVERSITÀ POLITECNICA DELLE MARCHE

Faculty of Engineering
Department of Information Engineering
Master of Science in Biomedical Engineering

Ethical Assessment Tools for Healthcare Information Technology and Application to Blockchain

Supervisor
Prof. Marco Baldi

Candidate
Giorgia Barchiesi

Co-Supervisor
Prof. Benedetta Giovanola

Academic Year 2021-2022

Abstract

Nowadays, any form of technology, applied in everyday life, is becoming one of the main subjects of philosophical and ethical reflection. Focusing on the healthcare field, the management of sensitive and personal data must guarantee the widest respect for patient's fundamental rights. However, even if ethics is one of the main topics of discussion, to date there is not any ethical evaluation framework which enables the achievement of a quantitative and objective assessment of the level of accomplishment of any technological infrastructure to the most important ethical pillars.

The purpose of this Master's Thesis is to provide an ethical evaluation framework able to produce a quantitative ethical adherence score of technological services in everyday life. In order to achieve this aim, a set of controls for the ethical features of Fairness, Privacy, Accuracy, Data Governance and Responsibility has been implemented, since, according to the literature, they represent the most important challenges of technology in healthcare.

Furthermore, starting from a qualitative overview of the most recent health-related blockchain frameworks, presented in the literature, a comparison between a qualitative ethical assessment and an objective ethical evaluation made using the proposed model, has been performed. As results, the highest final ethical score has been assigned to some technological infrastructures leveraging a permissioned blockchain and allowing an off-chain storage and encryption of processed data, contrary to the implementation of private blockchain with an on-chain storage mechanism, which obtains the lowest ethical evaluation score. Additionally, those ethical aspects which results to be satisfied by the majority of the analysed blockchain frameworks are Privacy and Data Governance, while, as observed from the qualitative analysis, the Fairness property results to be the hardest one to satisfy.

To conclude, this study could represent a starting point for further research, since it gives the first ethical evaluation model which is able to quantify the level of ethics of any organization in processing and sharing their data.

List of contents

List of figures

List of tables

Introduction

Nowadays, any form of technology, applied in everyday life, is becoming one of the main subjects of philosophical and ethical reflection. Focusing on the healthcare field, the management of sensitive and personal data, coming from diagnosis, treatment, medical services, or administrative operations, must guarantee absolute confidentiality and the widest respect for patient's fundamental rights. Indeed, in a completely digitalized world, health management, as well as other sectors, has been subjected to a dematerialization of documents, which has brought to the awareness that ethical behaviour should be the main topic of discussions and debates, as new technologies could run counter to many of its pillars. However, even if ethics is one of the main topics of discussion, to date there is not any ethical evaluation framework which enables the achievement of a quantitative and objective assessment of the level of accomplishment of any technological infrastructure to the most important ethical pillars. Starting from the definition of ethics, it is important to define two main aspects, which are the constitutive and the circumstantial perspectives. Specifically, the first terminology refers to the measure of the organization's level of adherence to the controls defined by a specific reference framework. These controls are useful to quantify which and how the main ethical pillars of Fairness, Privacy, Accuracy, Data Governance and Responsibility are satisfied and followed. On the other hand, the circumstantial ethical aspect is linked to the constitutive ethical assessment of the analysed frameworks, as well as, to their technical complexity. The latter is defined as function of the 15 essential cybersecurity controls defined by Research Centre of Cyber Intelligence and Information Security, and so, results to be directly linked with the increase of the probability of success of an adverse event.

Once of the difference between Constitutive and Circumstantial ethics has been specified, in order to face the impossibility of having an objective ethical assessment of the application of technology in everyday life, the purpose of this study is to provide an ethical evaluation framework able to produce a quantitative ethical adherence score of any technological applications.

In the last thirty years, with medical advances and the increased dynamics of clinical systems, the management of patient's health record is becoming one of the most relevant challenges faced by healthcare providers. In a context of increasingly complex and extended information systems, the blockchain represents, for the healthcare field, an element of innovation that provides an immutable and secure architecture for the management and the sharing of data within physically distant health

information systems. Specifically, the blockchain is a shared and immutable ledger that facilitates the transaction recording process and the traceability of assets in a commercial network. As the name implies, it is made up of many blocks, which contain a set of information collected in the system within a certain period of time. The blockchain, due to the way in which it transforms the interaction between the main actors of health systems and to its immutable structure, may appear to be in contrast with the main ethical pillars, such as Fairness, Privacy, Accuracy, Data Governance and Responsibility. The idea of making the use of blockchain technology compliant with the main ethical principles, highlighted in the literature, has prompted the analysis conducted in this work. So, after implementing the quantitative ethical evaluation frameworks, a set of the most recent blockchain frameworks proposed in the literature, has been considered as a case study, in order to compare the outputs provided by the quantitative analysis with a previous qualitative overview, and to evaluate similarities and differences of the final ethical assessments, together with an identification of how the quantitative analysis could improve the qualitative one.

In summary, by defining differences between the qualitative and the quantitative overviews, which aspects of the proposed blockchain frameworks are in common between those providing the best and the worst final ethical scores and which ethical principles result to be the easiest and the hardest to satisfy, this study could represent a starting point for further research, since it gives the first ethical evaluation model able to quantify the level of ethics of any organization in processing and sharing data.

CHAPTER 1

Ethics

1.1. General Features

Ethics is a branch of philosophy that "involves systematizing, defending, and recommending concepts of right and wrong behaviour" [1].

Frequently, normative ethical judgement depends on the adopted ethical approach. Indeed, in general terms, acts can be viewed from three perspectives: the agent who engages in the act, the act itself, and the consequences of the act. Traditionally, ethics dealt with transcendental values that were virtuous independent of the associated outcome or agents who acted in accordance with such values [2].

Applying the main definition of ethics in the healthcare field, it leads to the identification of some issues, which are becoming more complex with medical advances and the increased dynamics of the clinical system. Moreover, ethics studies can be divided into traditional ethics with well-known generic frameworks, and contemporary ethics with its specific environments and applications. The last years have seen the birth of many approaches for the assessment of the ethical impact of the emerging technology. The first study was conducted by Brey et al. [3], where a generic approach was proposed to identify the ethical problems by considering the inherent characteristics of the technology, the condition necessary for this realization and the impact that it can have. In addition to it, a second ethical technology framework was proposed by Palm and Hansson [4], which employs a control list of a set of ethical aspects covering the most critical issues related to emerging technologies. Finally, Stahl et al. [5] proposed a new approach to be followed when performing an ethical analysis, which included the identification of critical issues and the analysis of them based on law, philosophy and technological assessment [6].

1.2. Ethical challenges of Technology

In this chapter the attempt is to identify and evaluate the parameters of ethical challenges with technology application in e-healthcare.

The management of patients' health records is one of the biggest challenges faced by healthcare providers. Technology has transformed Electronic Health Records (EHR) by providing patient control over their medical data. Moreover, additional information such as timestamp, demographics, and signature are added to the records to facilitate easy retrieval. Since the technological approach for EHR has already found mainstream applications, some ethical consideration about its usage and application must be considered for its successful adoption. So, according to its application, various parameters for technology ethics have been evolved [7]. Among the ethical features identified there are:

- **Accountability**: it is a pillar of ethics, and it is defined both in terms of responsibility and liability. From a responsibility perspective, accountability requires that someone must account for what has happened and explain their actions, while from a liability point of view, it helps identify who should pay compensation if held responsible for an action. With the emerging of technologies, which involves both human and software, ethical behaviour needs to differentiate between accountability of software and humans.
- **Fairness**: it implies treating everyone equitably or reasonably. Even if the basic of peer-to-peer decentralized structure and the mode of operation of technology are designed to enforce non-discrimination and inclusion, they can also be used to consolidate and exert power over people and information.
- **Privacy**: it has been defined as the control an individual has over their personal information regarding how it is collected, processed, and used.
- **Accuracy**: it requires that personal data that has been collected should be correct. According to it, the zero-state problem represents the main issue to face. Particularly, the latter refers to the situation in which the veracity of initial items comes to question.
- **Right to be forgotten:** it allows people to exercise the right to erase or be forgotten from public databases after a certain period.
- **Data access**: it defines how a person can interact with and use any system. Indeed, it deals with the definition of what and how much information can be accessed, when will the access be permitted and who is permitted.
- **Data ownership**: it refers to the power given to users in having a full control over their data. However, the issues such as who owns the data and exercises control over how data will be stored and processed are the main ethical dilemma.
- **Governance**: it defines who is responsible for what, together with the mechanism of taking decision and implementing them.

Finally, according to the study in [7], which tried to evaluate the significance of these parameters in technology for healthcare, the Accountability, Data ownership and Governance ones do not make any ethical dilemma on the field of electronics health record (EHR) application.

Table I summarizes all the ethical parameters, highlighting if they are or are not a limitation for the application of technology in the healthcare sector.

Table I Ethical parameters in the application of technology in the healthcare sector

Parameters	***Healthcare Application (EHR and IoT)***
Accountability	No Ethical Dilemma
Fairness	Ethical Dilemma
Privacy	Ethical Dilemma
Accuracy	Ethical Dilemma
Right to be forgotten	Ethical Dilemma
Data access	Ethical Dilemma
Data ownership	No Ethical Dilemma
Governance	No Ethical Dilemma

CHAPTER 2

Quantitative Ethical Assessment

This chapter deals with a quantitative ethical assessment of the application of technology in healthcare. The evaluation is conducted through the implementation of two different ethical models, which enable an evaluation of both the constitutive and the circumstantial ethics of the previous analysed frameworks.

2.1. Definition of a New Ethical Evaluation Approach

Currently, there is a growing interest in the ethics of technology. Despite this, in the literature, there are few studies focusing on the impacts of technology on the moral field [8]. On this regard, the purpose of this study is to provide a new quantitative evaluation of technology ethics both from a constitutive and a circumstantial point of view, which are graphically described in Figure 2.1. To achieve this aim, two different models have been implemented. The first one concerns with an evaluation of a constitutive ethics index, which is determined through the implementation of a series of ethics controls. The second model deals with the computation of the probability that a successful attack may occur and with the definition of the circumstantial ethics of the framework considering the constitutive model together with the complexity of the implemented system. Indeed, the circumstantial ethical aspect is linked to the constitutive ethical assessment of the analysed frameworks, as well as, to their technical complexity. The latter is defined as function of the 15 essential cybersecurity controls defined by Research Centre of Cyber Intelligence and Information Security [9], and so, results to be directly linked with the increase of the probability of success of an adverse event.

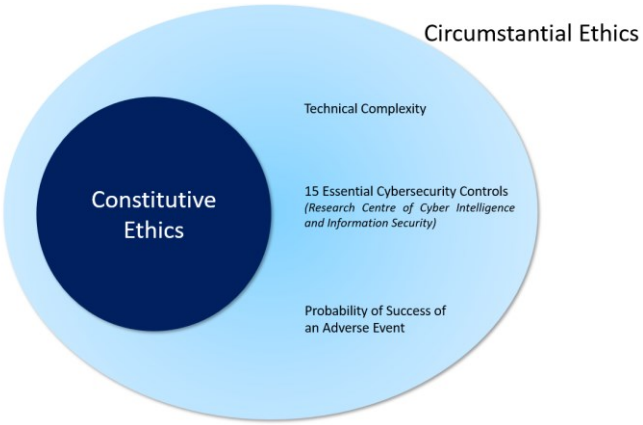


Figure 2.1 Definition of Constitutive and Circumstantial Ethics

Based on the cybersecurity assessments proposed in study [9], some key-concepts of this new framework, in addition to those mentioned above, will be the attractiveness of the analysed organization, the probability that an event occurs, and the context of application of system.

First of all, a *technical complexity index* has been computed starting from a set of controls which considers both the idea that the more a system tries to approach the ethical model, the more it will assume a complex internal structure - and so, the probability of success of an adverse event will increase - and the 15 essential cybersecurity controls defined by Research Centre of Cyber Intelligence and Information Security [9].

Secondly, the *constitutive ethics index* refers to the measure of the organization's level of adherence to the controls defined by a specific reference framework. Due to the lack of documentation on the ethical impacts of technology in the literature, nowadays, there is not an existing reference framework to consider. So, it has been constructed considering the main ethical challenges described in Chapter 2 and implementing, for each of them, a set of controls useful to build an evaluation checklist. The controls of the considered framework can be seen as complementary to the list of all possible threats. At the same time, the assessment of the constitutive ethics of the implementation of each control allows for an analysis of the vulnerabilities of the infrastructure. This idea is based on the concept that more an organization tries to enhance the level of adherence to an ethical assessment framework, more its technical complexity increases, and it makes the organization to be more vulnerable to a possible attack.

Finally, the concept of *attractiveness* is strictly related to the type of data managed inside the evaluated organization. Specifically, according to [11], if the importance given to ethics, and so the level of attractiveness of an organization, is directly proportional to the type of processed data, all those factors that positively influence a cyber-attack will increase. Moreover, the General Data Protection Regulation (GDPR) and ethics can be considered as two closely related concepts, since the importance given to ethical behaviour in processing and managing data is directly proportional to the GDPR data classification. So, according to it, dependently on whether an organization processes sensitive, personal, or other kinds of data, the attractiveness can be classified as High, Medium, and Low, respectively.

2.2. Constitutive Ethics Model

The constitutive ethics model is aimed to achieve an evaluation of the analysed frameworks considering the most important pillars of ethics. Specifically, with a checklist of controls and according to the answers chosen by the assessor through a drop-down menu, the ethical features of

Accuracy, Data Governance and Privacy, Fairness, Right to be Forgotten and Responsibility are quantitively evaluated.

2.2.1. Fundamental Structure of the Constitutive Ethics Model

The proposed model has been implemented in Excel, and it is made of different parts, which may need some inputs or provide outputs.

The first sheet is named "Cover", where the type of the organization is required to be selected and, according to the given answer, the model will associate a level of attractiveness, which depends on the type of processed data.

The second part of the model deals with an evaluation of the constitutive ethics of the organization, which is examined through a checklist of sub-controls to which a person can answer through a drop-down menu. Additionally, each sub-control belongs to a specific feature of ethics of technology in the healthcare field, such as *Accuracy, Data Governance and Privacy, Fairness, Right to be Forgotten and Responsibility*. For each sub-control, there is the possibility to choose one of the following answers:

- Yes, No or N/A: according to if the control is satisfied, not satisfied or not applicable
- High, Medium, Low or N/A: according to if the control requires to specify a certain degree of applicability of itself
- other kinds of answers: for example, when the control requires to specify if the type of classification used is anti-classification, classification parity, calibration, or statistical parity.

Finally, according to the given answer, a score is associated, which could be:

- 0, 1 or N/A if the choice is No, Yes or N/A, respectively
- 0, 0.5 or 1, if the choice is Low, Medium or High level, respectively

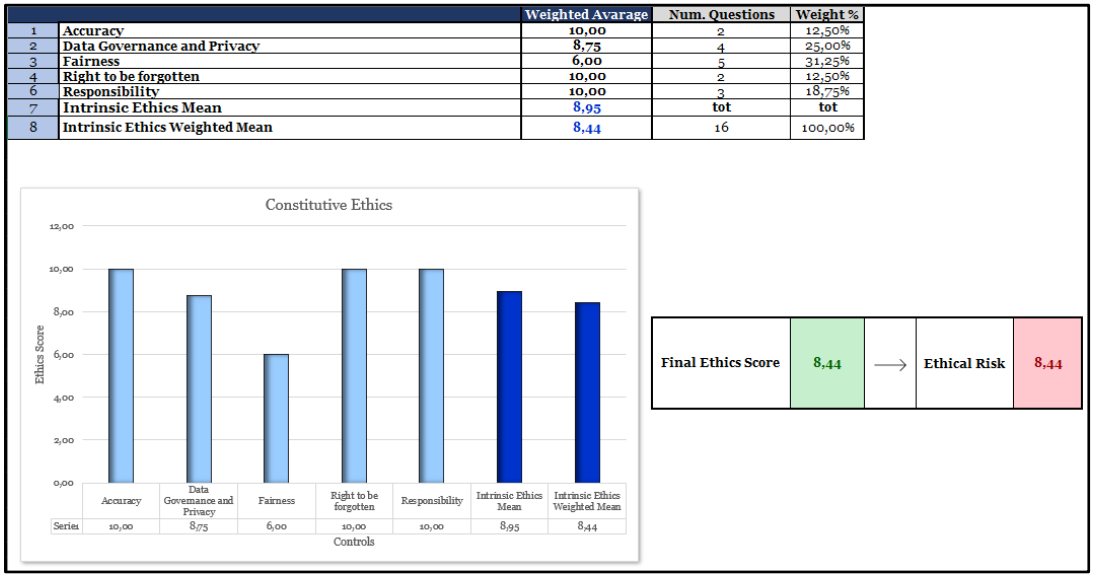
The output of this part is the weighted average of each ethics feature, computed according to the type of answers given to each sub-control and their corresponding weight.

After this evaluation is performed, a new sheet, called "Constitutive ethics index", summarizes all results obtained through the previous questionnaires. As shown in Figure 2.2, the sheet reports a summary table which indicates the values resulting from the assessment of ethics for each category. Additionally, there is also the assessment of the arithmetic average and the weighted average of ethics of the entire technological chain. In the same sheet, there is a histogram that graphically summarizes all the scores reported in the summary table together with the final ethics score and the computed ethical risk of the organization. Specifically, the first one correspond to the weighted avarage and is a value between 0 and 10, while, the second one is a score computed through the formula:

$$p = w \times P$$

where:

- P is the ethical weighted avarage
- w is the weight given by the type of the analysed organization and it can assume three different values according to the type of processed data (1 for sensitive data, 0.5 for personal data and 0 for all the others).



		Weighted Avarage	Num. Questions	Weight %
1	Accuracy	10,00	2	12,50%
2	Data Governance and Privacy	8,75	4	25,00%
3	Fairness	6,00	5	31,25%
4	Right to be forgotten	10,00	2	12,50%
6	Responsibility	10,00	3	18,75%
7	Intrinsic Ethics Mean	8,95	tot	tot
8	Intrinsic Ethics Weighted Mean	8,44	16	100,00%

Figure 2.2 “Constitutive ethics index” sheet of the Constitutive Ethics Model

2.2.2. Description of the Constitutive Ethics Model

The set of controls used in the evaluation questionnaire of the constitutive ethics model has been divided into different categories according to specific ethical features, such as *Accuracy, Data Governance and Privacy, Fairness, Right to be Forgotten* and *Responsibility*.

The first class of controls are related to the ethical challenge of **Accuracy**. Indeed, according to the study in [34], even if it is known how to ensure the validity of data once inserted in the system, there is poor information about how technology could provide a solution for the zero-state problem. On this regard, the two implemented controls are:

- *Every data is accompanied with a datasheet describing its operating characteristics* [8]: having a high level of knowledge about the source of the dataset or the assumptions under which sampling is done, it is possible to improve the transparency of data and so, the zero-state problem could be faced and reduced.
- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them* [8]: the possibility to interact with the system could be a crucial point to guarantee data accuracy and quality. Indeed, the correctness of data

could be analysed and evaluated by all those actors or nodes who can enjoy the network and visualize data.

The second set of controls have been implemented following the ethical concepts of **Data Governance and Privacy**, which could be difficult to follow due to the intrinsic structure of many technological infrastructures. Analysing these ethical features, three different controls have been implemented:

- *There is a system that avoids collecting or running a set of data if no consent has been given* [2]: this system is focused on improving the transparency of the decision-making process since, in big organizations, it is often opaque. Furthermore, this concept is related to the ethical perspective of deontology, as it allows anyone to focus on the duty of the individual in providing the evaluations of a given performance.
- *Evaluation of credentials of employees every time a new access is performed* [2]: the possibility to verify credentials and past performance could favour the use of technology in the recruitment and selection processes for the definition of entities that can enter and operate on the network.
- *Citizen's level of control over their data access and privacy* [12]: from the idea that ethics is needed to interpret existing legislation, such as the GDPR, or to recommend not to do something that legislation does not prohibit, this control is useful to determine who and how can access any kind of stored information. Specifically, three different levels of this control have been identified:
    1. *Low*: once data are inserted their processing follows specific ethical rules and the owner is no longer asked to confirm them.
    2. *Medium*: once data are inserted, their processing follows specific ethical rules, and the owner is asked to confirm them every time a new access is performed.
    3. *High*: once data are inserted, their processing follows specific ethical rules, and the owner is asked to confirm them every time a new access is performed. Additionally, there is the definition of who is authorized to visualize and modify data.

The third class of controls deals with the ethical challenge of **Fairness**, understood both as the absence of biases and discriminations, and as the concept of respect for individual person [13]. On this regard, the set of controls is made of:

- *The system complies with the Right to Justification* [13]: it means that the system does not allow any relationship or accounts if they are not adequately justified towards those involved. Additionally, every actor has the right to demand justification for the treatment he is subjected to.
- *The distribution of access to opportunities is not influenced by any form of contingencies* [13]: it refers to the opportunity for any person to express his agency and to the fair treatment of all users without any inappropriate form of discrimination linked to the role or social position.

- *Sensitive data are used to evaluate the necessity to acquire some compensatory tools* [13]: it is linked with the concept of access to opportunities since sensible data could reveal the presence of subjects who, in a certain domain, may require compensatory tools, such as supports or facilities.
- *Level of heterogeneity of the sources of used and analysed data* [8]: it underlines the importance of transparency of any set of data, which includes the knowledge about the sources, the assumptions under which the sampling has been done, or the used metrics. In this way, individuals may avoid the system to produce biases in the system outputs.
- *Type of classification used* [8]: the possibility to have a classification of individuals could avoid the presence of biases and improve decision-making processes.

The fourth group of controls deals with the **Right** for people to erase or **to be forgotten** from public databases. Since the intrinsic structure of some technologies does not allow any modification of data once they have been inserted, possible solutions to face this ethical problem are given by the following controls:

- *The use of sensitive data takes place in standalone systems disconnected from the network* [14]: it deals with the possibility to store data outside the network, giving the possibility to access them only once the consent has been given. Moreover, due to this kind of storage mechanism, it is always possible to delete or erase data.
- *Use of approved cryptographic mechanisms to protect stored data* [14]: it refers to the use of encryption for user verification, monitoring, data sharing etc. Additionally, the encryption of data also allows the possibility to erase them simply by throw away the secret key.

The last set of controls reflects the ethical property of **Responsibility**, meant as the enhancement to follow ethical guidelines. On this regard, the implemented set of controls is made of:

- *Level of accountability of participants and of any form of outcome of the system* [12]: any considered level refers to a different way of the system to identify who is responsible for a certain action. Specifically, these levels are:
  1. *Low:* the system has not any form of accountability process.
  2. *Medium*: there is a reward or penalty for any type of performed action and it is given to a group of participants.
  3. *High*: there is a reward or penalty for any type of performed action and it is given to a specific identified actor.
- *Type of responsibility implemented* [15]: it refers to the form of the responsibility relation between a subject of a decision or an action and the object of a decision or an action. The defined configurations are:
  1. *Monadic Responsibility*: it considers the general concept of responsibility.
  2. *Dyadic Responsibility*: it defines the responsibility for specific actions.

3. *Triadic Responsibility*: it defines the responsibility for specific actions towards somebody.

- *Volume of responsibility defined* [15]: it refers to the volume of the responsibility relation between a subject of a decision or an action and the object of a decision or an action. Specifically, the considered possibilities are:
  1. *Sole Responsibility*: only the owner of a decision is responsible for that
  2. *Shared Responsibility*: definition of specific category or group that is responsible for.
  3. *Sphere of Responsibility*: definition of specific types of situations in which a given person or group is responsible for.

2.3. Circumstantial Ethics Model

The circumstantial basic model aims to a quantitative evaluation considering not only the constitutive ethical assessment of the analysed frameworks, but also the technical complexity of the structure, which is directly linked with the increase of the probability of success of an adverse event, such as a cyber-attack. Indeed, when a system becomes vulnerable to an attack, the happening of the latter leads to data breach or leak and lower is the ethical behaviour of data management and storage, more will be the damage provoked by the attacker to the system.

2.3.1. Fundamental Structure of the Circumstantial Ethics Model

The proposed model has been implemented in Excel starting from the constitutive ethics model described in the previous section and adding two different sheets dealing with the technical complexity evaluation and index, and the computed risk.

The technical complexity evaluation concerns with a set of controls divided in three different categories, defined in studies [9] and [10], which are *Justice, Responsibility* and *Design*. Additionally, for each kind of control, there is the possibility of selecting the level of complexity of the system among Minimal, Low, Moderate, High, and Significant. This choice depends on five columns that guide the assessor to answer the questions, since their description are aimed to make the qualitative measurement as objective as possible. Then, a quantitative information is obtained associating a score to each answer. Specifically, for "Minimal" complexity the associated score is 1, for "Low" complexity, 2, for "Moderate" complexity, 3, for "High" complexity, 4, and for "Significant" complexity, 5. Finally, the average result is associated to a qualitative level of complexity:

- score <1.5→ Minimal
- 1.5 ≤ score <2.5 → Low
- 2.5 ≤ score < 3.5 → Moderate

- 3.5≤ score < 4.5 → High
- score ≥ 4.5 → Significant

After this evaluation has been performed, the “Technical Complexity Index" sheet reports its results. In this part there is a summary table reporting the values resulting from the evaluation of each category of controls. The table also shows the arithmetic average and the weighted one of the entire technological infrastructure. Particularly, the latter is computed as a ratio between the number of controls in each category and the total number of them. For convenience, and to facilitate understanding, scores are multiplied by 2 to obtain a decimal scale. In the same sheet, there is a histogram that graphically summarizes all the scores contained in the summary table. An example of both table and histogram is shown in Figure 2.3.

Technical Aspects Evaluation				
Technical Aspects	Level	Score	Num. Questions	Weight %
Justice	Moderate	6,29	7,00	46,67%
Responsability	Moderate	6,00	5,00	33,33%
Design	Low	4,00	3,00	20,00%
Complexity Avarage	**Moderate**	**5,43**	*tot*	*tot*
Weighted Avarage Complexity	**Moderate**	**5,73**	15,00	100%

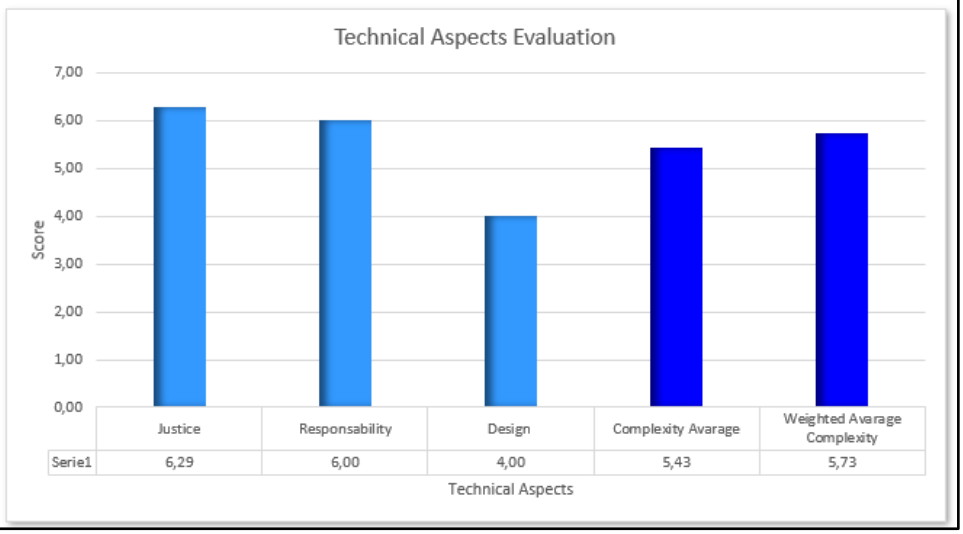


Figure 2.3 “Technical Complexity Index" sheet of the Circumstantial Ethics Model

After the evaluation of the technical complexity and of the constitutive ethics have been performed, all the necessary inputs have been provided and it is therefore possible to proceed with the risk assessment in the last sheet of the model, which is shown in Figure 2.4.

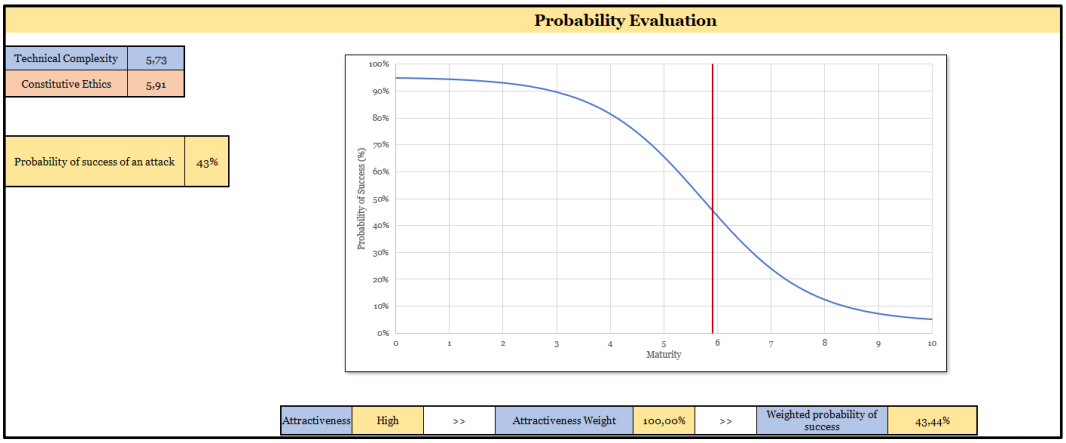


Figure 2.4 "Computed Risk Assessment" sheet of the Circumstantial Ethics Model

At the beginning of the window there are the technical complexity index and the constitutive ethics value, which results from the answers given to the checklists of controls presented in the previous sheets. The reason why these two scores are reported is that the probability of success of an adverse event is influenced by the attractiveness of the organization, the technical complexity of the infrastructure and its level of adherence to the proposed ethical evaluation framework. Specifically, technical complexity and the probability of success of an attack result to be directly correlated since more an organization is complex from a technical point of view, more it will be vulnerable to a specific type of attack. On the other hand, higher is the constitutive ethics index of an analysed organization, lower will be the probability that an attacker success in its attempt. So, based on the idea that technical complexity and constitutive ethics indexes influence the probability of success of an adverse event, in the same sheet is also reported the curve of the generalized logistic function, defined in study [9] through the formula:

$$y(t) = A + \frac{K - A}{(1 + Qe^{-B(t-M)})^{1/\nu}}$$

where:

- A is the lower asymptote, which determines the minimal value of the curve;
- Q is a variable dependent on $f(x_0)$, which affects the inflection point;
- x_0 is the point in which $f(x_0) = A + \frac{K-A}{(1+Q)^{1/\nu}}$;
- $\upsilon > 0$ determines the asymmetry of the curve;
- K is the saturation level, that is the superior horizontal asymptote, which determines the maximal value of the curve;
- B is the rate of growth, which determines the slope of the curve.

In the proposed model Q and ν are fixed equal to 1 to make x_0 be the point of maximum growth of the curve. Since the constitutive ethics and the probability of success are inversely correlated (an increase of the first term corresponds to a lower probability of success of an adverse event and vice

versa), a negative growth rate ($B = -1$) has been considered. The variable x, which represents the constitutive ethics of the infrastructure, is normalized in the range between 0 and 10, extremes included. Furthermore, it is assumed that the probability of success does not reach the extremes 1 and 0 in the finite regime. This is because in real infrastructures, even in the worst case, there is always a non-zero probability that no harmful events will occur and, vice versa. Indeed, even when the maturity index reaches its maximum value, it is not possible to exclude the possibility of an adverse event occurring. On this regard, to represent this condition in the model, the maximum and minimum values of the curve are set respectively at 0.95 for $x = 0$ and at 0.05 for $x = 10$. In this way, the values of K and of A depend on the value of x_0 and they can be easily obtained by solving the following system:

$$\begin{cases} f(0) = A + \dfrac{k - A}{1 + e^{-x_0}} = 0.95 \\ f(10) = A + \dfrac{k - A}{1 + e^{(10 - x_0)}} = 0.05 \end{cases}$$

Another parameter that is considered in the proposed model is the attractiveness of the organization, which depends on the type of processed data. Therefore, different types of organizations have different attractiveness and, consequently, are exposed to different levels of risk. Therefore, in the proposed model, the previously obtained probability of success (P) is weighted according to the attractiveness of the organization through a simple weighting of the following type:

$$p = wP$$

where:

- P is the probability of success of an attack;
- p is the weighted probability of success of an attack;
- w is the weight, which could be 1, 0.5 or 0 according to if the type of processed data are sensible, personal or others, respectively.

Finally, to estimate the probability of having exactly one successful attack, the probability calculation is stopped as soon as an attempt is successful. This corresponds to the use of a geometric distribution. The geometric distribution in fact provides the statistical distribution of the exact number of failures preceding the first successful attack. As computed in study [9], let p be the probability of success of a single attack attempt, the probability that the first success occurs after $i - 1$ failures, under the hypothesis of statistical independence of the attack attempts, is given by the following expression:

$$L(i) = (1 - p)^{(i-1)}p$$

2.3.2. Description of the Circumstantial Ethics Model Controls

The set of controls used in the evaluation checklist of the constitutive ethics model is divided into different categories according to specific technical aspects.

The first class of controls is related to the concept of **Technical Robustness and Safety**, and it includes:

- *Definition of a range of human abilities, skills and requirements needed to access to the technological infrastructure* [9]: it is linked with the assumption that the trustworthiness and the security of a system are mainly based on the definition of the main user characteristics. Here, increasing the level of knowledge associated to any user participating in the network, also the level of complexity of the system is enhanced.
- *Implementation of a technique to make the system relevant over time* [16]: the fact that the system is relevant over time considers the evolutions that it can assume. For this reason, any specific way of reorganization is associated with a single level of technical complexity.
- *Implementation of a technique to make the system secure over time* [12]: it considers the idea that the security of a system is linked not only to the level of protection towards any type of data access, but also to the possibility of selecting only the necessary data that can be visible to users.
- *Definition of the level of resilience of the system to an attack* [17]: it describes the ability to continue to deliver the expected results despite the occurrence of challenging cyber events, such as cyber-attacks. To achieve this purpose, different protection techniques to be implemented, have been considered [18] [19] [20]:
    1. *Intrusion Detection System*: based on the assumption that the behaviour of an intruder differs from that of a legitimate user in ways that can be quantified through statistical approaches or audit records.
    2. *WPA* (Wi-Fi Protected Access): is a protocol created to generate secure Wi-Fi wireless networks thanks to data encryption. There are some advances of this type of protection system, which are
        - *WPA2*: it is more secure than WPA. WPA2 requires the use of stronger wireless encryption than WPA, and consequently improves the security of Wi-Fi connections.
        - *WPA3*: when the user connects via mobile device to a public or private Wi-Fi network, every single connection will be encrypted. Additionally, it is no longer necessary to enter the network password to access the encryption. Any connection, even those to open wireless networks that do not require a password, will still be protected.
    3. *Authentication Protocols*: they refer to processes of validation of the authenticity of a client. Specifically, they are divided int a series of protocols, which are:

- *Extensible Authentication Protocol (AEP)*: it involves three components (peer, authenticator, and server) providing a basic request/response structure which support authentication credentials such as challenges, password, certificates, and keys.
- *Password Authentication Protocol (PAP)*: it deals with sending credentials to the authentication server in an unencrypted way. The basic flow of this process includes the login request, the challenge, and the access permission.
- *Challenge Handshake Authentication Protocol (CHAP)*: it depends on a secret challenge known only by the authenticator and the peer. Once achieved the last step of the authentication flow, if the result of the proposed challenge marches, the authentication is successful, otherwise everything starts again.
- *Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)*: it works encrypting password information before the communication starts and then, all the authentication steps and challenges can start.

4. *Network Security Protocols*: they are used to allow a secure communication over network. Among them there are protocols which deal with general data transmission, such as the Transport Layer Security (TLS). The latter is a standardization of the Secure Socket Layer (SSL), and it is based on a peer-to-peer connection, and it is temporary and associated with the established session communication. Next to it, another example can be the Virtual Private Network (VPN), which aims to make secure the network infrastructure against unauthorized use and control the network traffic by using authentication and encryption.

- *Definition of the level of accuracy, reliability, and reproducibility of data* [21]: starting from the idea that the technical complexity of a system is directly proportional to the level of accuracy of the inserted data, different levels of reliability have been specified:
    1. *Very Low*: there are no references regarding entered data.
    2. *Low*: data are accompanied by a qualitative temporal and personal description of the subject.
    3. *Medium*: data are accompanied by a qualitative description on the methods used to carry out the detection of the signals.
    4. *High*: interactive interface in which inserted data can be validated by the owner.
    5. *Very High*: interactive interface in which data can be validated by the owner and there are also measurements regarding the context of use, rules, characteristics, and constraints of the reference business.
- *All devices are equipped with regularly updated protection software (antivirus, antimalware, etc...)* [9]: a malware is defined as any software that, once executed on a computer system, can

make unwanted changes or damage to the system and its users. The use of anti-malware software is necessary to protect devices from attacks.

- *Definition of the initial configuration of the systems and backup* [9]: to ensure the availability of all the data, configurations, and information critical for the proper functioning of the company, the organization must also have an appropriate backup strategy that allows for rapid and effective recovery in the event of an accident. Backups must be carried out on a periodic basis, defined according to the specific needs.

The second classification is based on the **Identification** property of a system technology. Specifically, it is based on the idea that it is important to have a clear definition of who can access data, which kind of data can be seen or processed, and how it can be done.
The set of controls forming this second category is made of:

- *An inventory of the systems, devices, software, services, and IT applications in use within the company perimeter exists and is updated* [9]: the number of devices that today can be vehicles for cyber-attacks is enormous: not only PCs, smartphones, and tablets, but also surveillance cameras, smart-TVs, etc. Only authorized devices should be able to access the network, and it is necessary to ensure that unauthorized and unmanaged devices can be readily identified so that they are prevented from accessing. It is therefore essential, in order to establish a good IT security management policy, to create an inventory of all those devices that in some ways are part of the company or of one's digital life.
- *Total number of external connections (social network, cloud computing, email, website)* [9]: it is linked with the idea that the number of connections can directly influence the complexity of the technical structure of the organization since each of them should require the identification of resources and a process of managing users (accounts). So, a good practice is to delete or deactivate accounts that are no longer used since they may contain important information.
- *Critical information, data and systems for the company are identified so that they are adequately protected* [9]: bearing in mind that failure to protect these assets could result in sanctions, economic losses, business interruption, or loss of competitive advantage, data and information must be classified according to a criterion that considers their criticality (e.g., public data, data for commercial use only, confidential data, secret data, etc.).
- *Definition of the roles of IT network personnel* [9]: it is necessary for the company to appoint a person in charge of coordinating the management and the protection of information and IT systems.
- *The laws and/or regulations with relevance in terms of cybersecurity that are applicable for the company are identified and respected* [9]: starting from the idea that any implemented

law influences the organization's level of technical complexity, the following classification has been identified:

1. *Minimal*: use of an IT authentication system, through the assignment of authentication credentials (the secrecy of which must be ensured) and the adoption of procedures for the custody of access devices and security copies, in order to guarantee the restoration and the availability of data and systems.
2. *Low*: use of an authorization system, by limiting the access to only the data necessary to carry out the processing operations, the identification of authorization profiles and the periodic verification of the conditions of existence for the conservation of these authorization profiles.
3. *Moderate*: implementation of other security measures, such as the preparation of a list of persons in charge for homogeneous classes of assignment and the related authorization profiles, the saving of data at least weekly and the periodic updating of programs aimed at preventing the vulnerabilities of electronic tools.
4. *High*: further measures in the case of the processing of sensitive or judicial data, whose restoration and access must be guaranteed in case of damage, and which must be protected using suitable electronic tools and adequate procedures related to the custody and the access from not directly authorized persons.
5. *Significant*: use of protection and guarantee measures, which provide the possibility using subjects external to the structure, which certify compliance with the provisions described above.

The last group of controls is linked with the analysis of **Online Services**. On this regard, if from one side online services could facilitate communication and make the exchange of information faster, on the other hand they make the technical part of any system or organization more difficult to realize. The controls in this section are:

- *Interaction and integration with social media* [10]: considering that the complexity of the organization depends on the possibility to use or not social media together with their continuous growing diffusion in today's world. This control aims to underline that the possibility to use the online services could not only facilitate the communication with the consumer, but it could also enhance the complexity of the organization
- *Provision of online services (including extranet)* [10]: the amount of provision of online services makes the complexity of the entire examined organization increase.
- *Provision of services on Mobile (including extranet)* [10]: as described in the previous control, the possibility to have services on Mobile is also directly proportional to the complexity of the organization.

CHAPTER 3

Blockchain Technology

3.1 General Features

Proposed by Satoshi Nakamoto in 2008, a blockchain is a distributed ledger for tracking transaction between parties [22]. As the name implies, a blockchain is made up of many blocks, which contain a set of information collected in the system within a certain period of time. So, a block constitutes the basic unit that forms the distributed ledger, and it has its own timestamp, which represents the unique mark to ensure the traceability of the blockchain. Moreover, each block is divided into two parts: Block Header and Block Body. The first contains the link pointers to the previous block, the Merkle root tree[1] [22], and a timestamp, while the second one is involved in the recording of all data information in the network. In this way, blocks are linked together in a chronological order, and they are uniquely identified by a hash value computed through the Secure Hash Algorithm (SHA-256). So, each block contains its own cryptographic hash together with the hash owned by the previous one. This is true for all blocks of the blockchain excepts for the first one, which is created from scratch [23, 24]. The single block structure and the way in which these single elements are linked are shown in Figure 3.1 [25, 26].

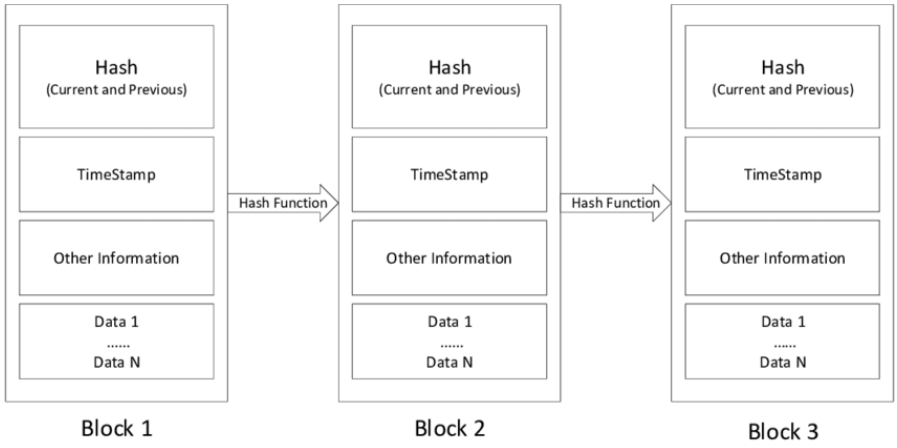


Figure 3.1 Blockchain Structure

[1] The Merkle Tree is a data structure, which allows the storage of all cryptographic hash of transactions in the block. It is created by hashing pair of nodes in a tree until a single hash is left, which takes the name of Merkle root.

Generally, a blockchain has the following properties [27]:

- Decentralization: that is the elimination of the involvement of a third-party entity, which is no more needed for processing data and maintaining a record. All transactions are validated and executed after the agreement of the majority of the participants has been given.
- Immutability: due to the structure of each block and to the link present between a block and its previous one, if a malicious entity attempts to tamper with a data, the hash of the block will change. Consequently, the attacker should rehash all the subsequent blocks in the chain, and this is a too high compute-intensive work which leads to the immutability of the entire system.
- Transparency: it is linked with the possibility to access data, which results to be completely allowed in case of public blockchain frameworks.
- Traceability: it is due to the ability of the blockchain to store all the transaction history without giving the possibility to erase or modify it.
- Consensus: it is given by the fact that each transaction in the blockchain is performed after a form of common agreement of most of the participants has been given.
- Trust: it is given by the cooperation between governance rules, cryptographic tools, and immutable transactions.

3.2. Types of Blockchain

Blockchain technologies can be classified depending on the implementation design, administration rules and access permissions. Particularly, they can be classified as “public” and “private”, as well as, in terms of “permissioned” and permissionless” [28].

Particularly, there are [28]:

- Permissionless Public: anyone can join or leave the network, maintain the ledger, and participate in consensus mechanism. Therefore, it provides minimum trust among the participants while achieving the maximum transparency.
- Permissioned Public: anyone can read the blockchain data, but only permissioned nodes have the possibility to write.
- Permissioned Private: there is the implementation of a permissioned access control system applied to data storage and controlled occurs by users of the network.

Additionally, permissionless public blockchains are referred to as public blockchains, while permissioned private blockchains are called private. On the other hand, a combination of permissioned public and permissionless private forms a “consortium blockchain” [28].

3.3. Transaction

Due to its distributive nature, blockchain allows decentralized transactions between nodes. Particularly, a transaction is designed as dome data stored in a single block, so, after its recording, this kind of information exchanged becomes unmodifiable and cannot be tampered once it is placed inside the distributed ledger. Moreover, the block body is composed of a transaction counter and transactions and their size determine the number of transactions that a block can contain. In Figure 3.2 the entire block structure is represented.

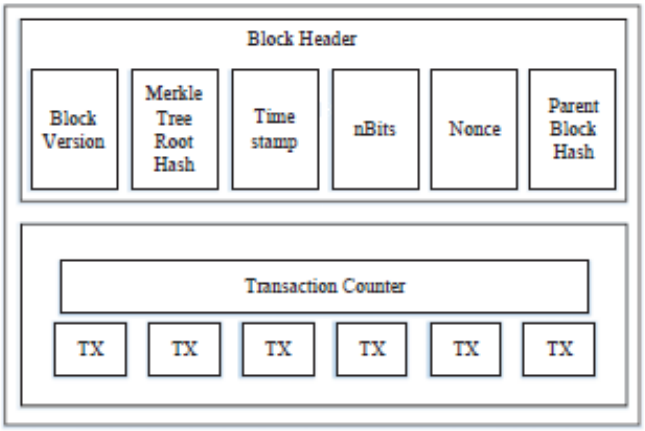


Figure 3.2 Block Structure

Finally, the validation and authentication of each transaction is performed through the implementation of an asymmetric cryptographic mechanism. Indeed, each user owns a pair of private and public key, where the first one is kept secret in order to be used for the digital signature. After a transaction has been signed, it is sent throughout the whole network.

Regarding the digital signature, it is made of two different phases:

- Signing phase: where the sender encrypts his data with his private key and gives it, together with the original data, to another user
- Verification phase: where the receiver validates the value with the sender's public key and checks if the data has been tampered or not.

In summary, according to the blockchain structure, the key characteristics of each transaction are:

- Decentralization: their validation is not performed by a central trusted authority but is the result of the implementation of a consensus algorithm.
- Persistency: only validated transactions are admitted inside the blockchain structure, while the invalid ones are not accepted by honest nodes.

Finally, according to the type of blockchain implemented (private, public or consortium), there are some transactions' application that may vary. For example, according to the reading permissions, transactions in a public blockchain are visible to everyone, while it is not true where they come to a private blockchain or to a consortium one. Moreover, since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain. Differently, transactions in a private blockchain or a consortium blockchain could be tampered in an easy way as there are only a limited number of participants [29].

3.4. Mining and consensus mechanisms

The process of creation of new blocks is called "Mining" and it is realized by means of entities belonging to the network, which are known as "Miners". The creation of a new block is linked with the necessity to identify the type of transaction, the selection of the last block of the chain together with the hash of the new block, and the solution of a Proof-of-Work (POW), which ensure the validity of the blocks. Indeed, each block is the result of a specific type of proof, which is a-priori identified and it must be used for any basic unit of the blockchain technology. Specifically, the implemented proof can be the Proof-of-Work, the Proof-of-Stake (POS) or the Proof-of-Burn.

The first one, it is a consensus strategy which aims to select a node to record transactions. Even if the easiest way could be the random selection, it results to be vulnerable to attacks. So, when a node wants to publish a block of transactions, it must perform a lot of work in terms of computer calculations. Indeed, at this stage, miners continuously try to solve cryptographic puzzles in the form of hash computations by using the hash algorithm SHA-256, whose output is unpredictable, and it allows to create a new block by means of a set of attempts aimed to find a lower hash value with respect to the target one [27, 30].

Regarding the Proof-of-Stake, it is an alternative to the POW, where miners must prove the ownership of a specific currency, since the probability that a node attacks the network is inversely proportional to the amount of currency owned. Moreover, compared to POW, POS saves more energy, and it is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. This is the reason why many blockchains adopt POW at the beginning and transform it to POS gradually [27, 31].

Finally, the Proof-of-Burn distributes the right to mine according to the "sacrifice" done, which means that the miner's possibility of being selected to extract the next block is proportional to the number of coins invested in an irretrievable way [32].

Next to these types of proofs, there are also other blockchain system implementations based on different consensus mechanism like Round Robin and Practical Byzantine Fault Tolerance (PBFT), which aim to achieve a common agreement about the newly added block of the ledger.

Specifically, Round Robin restricts the mining process only to those entities which are identifiable, while the PBFT subdivides nodes into primary, which announce the transaction, and secondary, which sign the transaction to verify it. So, PBFT requires that every node is known to the network [33, 34].

Finally, as shown in Table II, these consensus algorithms can lead to significant advantages and disadvantages according to the types of implemented proof. These positive and negative characteristics deal with:

- Privacy protection of data
- Number of nodes needed for computing the consensus mechanism
- Amount of cost for the proof computation

Particularly, as showed in Table II, PBFT results to allow a higher privacy protection together with lower computing costs due to the use of a smaller number of nodes.

Table II Performance Comparison between the proposed and the confirmed approaches

	Privacy Protection	**Fewer number of nodes**	**Less computing cost**
Proof of Importance (PoI)[2]	🔴	🔴	🔴
Proof of Work (PoW)	🔴	🔴	🔴
Delegated Proof of Stake (DPoS)[3]	🟢	🔴	🟢
Practical Byzantine Fault Tolerance (PBFT)	🟢	🟢	🟢

[2] Blockchain consensus mechanism used to determine which nodes are allowed to add a block basing on an evaluation of their importance over the blockchain network

[3] Blockchain consensus mechanism where block validation is executed by delegates, which are elected based on their reputation.

3.5. Ethereum

Ethereum is a public blockchain with a basic programming language, which allows to write programs that can solve any reasonable computational problem. So, it can be seen as an alternative protocol for the building of decentralized applications, which are named smart contract. Due to its self-executable nature, a smart contract allows to accomplish several important tasks, such as an improvement of security of any application system, a rapid development in time and an interoperability mechanism [35].

For what concern Ethereum accounts, there are two different types of them, called externally owned accounts, which are controlled by private keys, and contracts accounts, which are controlled by codes. Additionally, each of them is provided with a 20-byte address and contains four different areas [36]:

- Nonce: if the account is an externally owned one, this number represents the number of transactions sent from the account's address. On the other hand, if the account is a contract account, the nonce is the number of contracts created by the account.
- Balance: The number of Wei owned by each account. Specifically, a Wei is the smallest allowed fraction of Ether, which is the virtual currency.
- StorageRoot: it is a 256-bit hash, which allows to encode the storage contents of the account.
- CodeHash: it is the code that is executed when the corresponding address receives a message call. It is immutable and thus, cannot be changed after its construction.

Figure 3.3 shows the two types of Ethereum accounts, together with their components.

Figure 3.3 Types of Ethereum Accounts

To conclude, Ethereum, taken as a whole, can be viewed as a transaction-based state machine, where, at the beginning, a genesis state is generated, and then, through the execution of transactions, a final state is achieved. When it happens, it can be said that this final state is the canonical version of the world Ethereum. Moreover, the state can include a series of data, such as account balance, trust arrangements, data coming from the physical world and any other kind of information which can be easily represented by a computerized machine [37].

CHAPTER 4

Blockchain in Healthcare

In a context of increasingly complex and extended information systems, the blockchain represents, for the healthcare field, an element of innovation that provides an immutable and secure architecture for the management and sharing of data within physically distant health information systems. Nowadays, different types of blockchain-based systems have been implemented and this chapter aims to define the main characteristics of the most recent blockchain frameworks in literature. According to literature, in recent years, several types of Healthcare Blockchain Frameworks have been proposed. Here, the following recent blockchain frameworks are analysed:

- DITrust Chain [25];
- CP-BDHCA [38];
- HealthBlock [39];
- MEXchange [40];
- Mukesh et al. proposal [22];
- hOCBS [41];
- MedicalChain [42];
- MedRec [43];
- Akbar et al. proposal [44];
- Sun et al. proposal [26];
- Truong et al. proposal [45]

4.1. DiTrust Chain

Healthcare based Internet of Things (IoHT) are systems that collect information from different sensing devices using middleware. Moreover, IoT and its applications are becoming an integrated part of everyday lives and it is due to the necessity to accelerate the integration between the physical and virtual worlds. This technology will play an important role in the remote monitoring of patients in hospitals but, above all, at home [46].

Proposed by Eman M. Abou-Nassar et al. in 2020, DITrust Chain allows a privacy-aware management framework to preserve sensitive data of patients improving security and interoperability mechanisms [25]. The DITrust Chain is designed to generate secure cooperative IoT zones with

reliable information between its members. Moreover, the considered model, uses two types of Blockchain technologies i.e., the public blockchain, which connects every object to the network environment, and the ripple one, which is a permissioned system limiting the access to available information. For the implementation of the considered model, an evaluation of the security issues is conducted, and the main features considered are:

- *Scalability*: it is defined as the capacity to guarantee that the framework size has no effect on its performance. Since in the DITrust Chain there is the presence of a Public Blockchain to cover the aggregation request, the considered model is seen as a scalable one.
- *Mutual authentication*: since in the proposed framework each gadget has an ID plate[4] signed by its primary key, the legitimacy of any member is always verified.
- *Privacy*: it is realised using the Ripple chain, which, due to its permissioned structure, makes transactions available only to validated nodes.

4.2. CP-BDHCA

Healthcare Big Data (HBD) allows to analyse, access, and retrieve personal and electronic healthcare records (EHR) of patients. Frequently, the storage of these records is subjected to personnel latency, security, and privacy risks. A possible solution to achieve a faster analysis together with a secure storage is the one proposed by Ghayvat et al. in 2021 [38]. It is a blockchain-based confidentiality-privacy scheme, CP-BDHCA, which operates in two phases. In the first one, the session key establishment is done, and once keys are determined, the asymmetric key pairs generation takes place to secure the HER access. The entire flow of the system is shown in Figure 4.1.

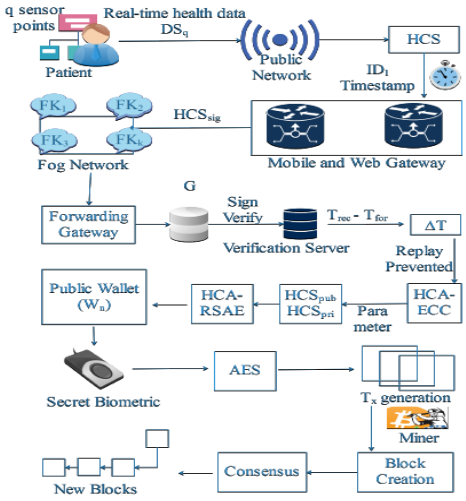


Figure 4.1 CP-BDHCA: the system model

[4] Structure which uniquely identifies a primary object. It is made by the member ID, the group ID, the public address and the private tag.

Considering a certain number of IoT sensors applied on a patient, named $\{S_1, \ldots, S_q\}$, the server generates real-time health data, D_{Sq}, and sends them to a healthcare cloud server (HCS) over the public network, which generates digital timestamps of the received data. Then, data are transmitted to k fog sensors nodes[5], named $\{F_1, \ldots, F_k\}$, through the mobile and web gateways, $\{G_m, G_w\}$. They also allow data encryption with the symmetric Key K_s. At HCS, the verification of identity of G_m and G_w is done, and the received and forwarded timestamp T_{rec} and T_{for} are recorded. At this point, their difference is stored since it becomes useful to face replay attacks.

Once data verification is done, the key establishment phase starts using an elliptic curve cryptographic-based digital signature framework (HCA-ECC). This cryptographic system is like RSA public key but allows the use of smaller keys with a security that depends on the difficulty to compute the elliptic curve discrete logarithmic problem [47].

Then, for the access control, the integration of Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) is computed, generating a scheme called HCA-RSAE. Here, the generation of secure key pairs is performed to allow communication between authorized entities.

4.3. HealthBlock

Proposed in 2021 by Zaabar et al., HealthBlock is aimed to enhance the security and privacy of EHRs by using blockchain technology [39].

The architecture of the system is shown in Figure 4.2, and it is composed of six layers:

1. The first layer is the physical one and consists of wearable health devices, which aim to capture real-time patient vital signals.
2. The second layer is the connectivity one and includes ways to allow the communication of vital signals to healthcare IoT servers.
3. The third layer is the off-chain database one, which produce hash values of data and sends them to the blockchain database.
4. The fourth layer is the blockchain network one, which is permissioned allowing the access only to authorized users.
5. The fifth layer is the application one, which provides a remote patient monitoring
6. The sixth layer is the users one, which consists of patients and physicians who interact with the blockchain interface

[5] Fog Computing refers to a layered service structure composed of low-energy computing nodes, which can provide faster storages and computations, since they are located near the devices at the edge of the network [6].

Figure 4.2 HealthBlock architecture

Furthermore, the HealthBlock uses two blockchain channels:

- *Medical devices blockchain channel*: it is used by patients and physicians to handle wearable health devices status
- *Consultation blockchain channel*: it is used by patients and physicians to control access to patient's healthcare data

Finally, with this model, security and privacy requirements are satisfied. Particularly, data integrity is achieved by encrypting and storing them in a decentralized database and inserting their hash values into the blockchain. Moreover, confidentiality and privacy are given by implementing a permissioned blockchain, where access is allowed only to authorized participants. So, according to these features, the HealthBlock system provides a high immutability level and contributes to create a patient-centric access control for sensitive and personal data.

4.4. Mexchange

Proposed by Lee et al. in 2021, MEXchange is a blockchain-based model that solves privacy issue by obscuring the sender and receiver addresses [40].The scheme of this model is made up of four players:

- *Certificate Authority*: it authenticates new participants and records them in the blockchain
- *Hospitals*: they manage health information in databases
- *Patients*: they grant access to the requestors and exchange health information
- *Requestors*: they ask patients for access and request health information from hospitals.

Moreover, security and privacy are enhanced by employing a private permissioned blockchain and using ring signature and stealth addresses. Specifically, a ring signature is a type of digital signature

which can be performed by any member of a specific group. Indeed, a ring signature is like a group signature, which makes infeasible to determine which member signs a specific document. As shown in Figure 4.3, MEXchange components are divided into three layers:

1. *Presentation layer*: it is the user interface for interacting directly with other endpoints.
2. *Business Logic layer*: it connects the presentation layer with the storage one.
3. *Storage layer*: it manages the data required to operate MEXchange.

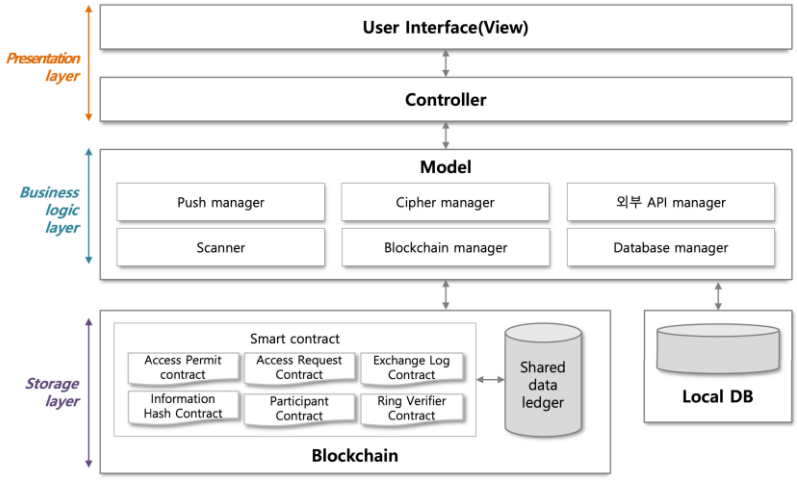


Figure 4.3 MEXchange Structure

Conclusively, MEXchange presents the disadvantage of increasing transaction latency. However, it shows several important strengths such as:

- *Confidentiality*: since data are stored in an encrypted way, only authorized users can access them
- *Integrity*: data are managed inside the blockchain, which makes impossible any modification
- *Privacy*: addresses are obscured by using ring signatures

4.5. Mukesh proposal

Proposed by Mukesh in 2021 [22], this approach incorporates blockchain, smart contract, zk-SNARK[6], and encryption techniques to improve healthcare data exchange between patients and medical institutions. In this model there are seven organizations involved:

- *Patients*: they can own and share their health data
- *Hospitals*: online medical records are provided to them
- *Research institutions*: they use medical records for clinical research

[6] "Zero-knowledge" proof, where the prover can demonstrate to the verifier that a statement is true without reveal anything about its content.

- *Private Key Generation*: involved in the creation of private and public keys shared between patients, hospitals, and research institutions
- *Blockchain*: where data are stored
- *Smart contract*: used for the verification of data
- *Semi-trusted proxy cloud server*: stores and decrypts the original ciphertext

The implementation of the model starts with the private key generation, which allows a secure data sharing among parties. Then, data are encrypted and stored in the blockchain. At this point, for a person to generate the zero-knowledge proof on his data, he needs to apply a digital signature so that it can be accepted as evidence.

4.6. hOCBS

Proposed by Miyachi et al. in 2021, hOCBS [41] refers to a hybrid Off-chain Blockchain System based on patient-centric and privacy-preserving approaches to manage three types of healthcare data: Protected Health Information (PHI), Consumer Health Information (CHI) and Genomics Data.

Protected Health Information is defined as any information in a medical record that can be used to identify an individual and to provide a healthcare service. The blockchain model used for this type of data focuses on the management of them involving legally classified organizations and patient-centric control over the network. In this model, to improve security, authentication and authorization processes are executed both for data access and modification. Furthermore, cryptographic techniques are used to validate information on a connected database.

Consumer Health Information concept refers to any information on health and diseases that is created and directed to public. So, this second model focuses on the control and sharing of this kind of data which provides a consumer-centric control, and which is subjected to general privacy frameworks such as GDPR. Here, security is guaranteed by allowing data sharing only after a proper authentication and authorization from the consumer.

Genomics Data define all data about a person's gene, which is considered as a growing form of health-related information. For this reason, an off-chain storage approach is used, since it can work with a larger volume of data. In this model, security is added by verifying the owner approval of its own data sharing while maintaining anonymity.

Finally, among the main benefits for hOCBS architecture there are the possibility of sharing and process a large amount of data, the reduction of storage requirements, the development of privacy-preserving mechanism such as anonymity.

4.7. MedicalChain

Proposed in 2018, MedicalChain [42] is a decentralised platform which enables a secure and fast exchange of medical data over the network. Its structure is based on a dual blockchain usage, where the first one is developed to control access to any patient data, while the second one is linked with the application of an Ethereum underlying the series of applications and services allowed for the used platform. Additionally, this type of blockchain framework is built on a permissioned- based Hyperledger Fabric architecture, which represents a solution for managing access to health records since each owner can control which parts of its data are accessed.

One of the massive problems in the digital world is the presence of identity fraud since hackers are able to impersonate users to tamper data and incur huge costs. So, to face this phenomenon, MedicalChain operates with Civics' user authentication services to manage the identities of all nodes by using biometrics, which also represents a way to ensure users privacy. Moreover, this ethical aspect is provided by the implementation of a symmetric key cryptography. Particularly, when an entity is allowed to access the patient's record, the latter is decrypted with the owner's private key, while the symmetric key is encrypted with the public key of the authorised user. On the other hand, each time a participant's access is removed, the symmetric key is decrypted with the private key of the patient, and it is used to decrypt the health record, which then is re-encrypted with a new symmetric key and the latter is encrypted with all the remaining users' public keys.

In conclusion, this decentralised platform enables users to give conditional access to different healthcare agents such as doctors, hospitals, or pharmacists and, additionally, it shows some key features, such as:

- User control: the user is the owner of their own medical records
- Data security: guaranteed through the implementation of a double encryption mechanism on a permissioned blockchain
- Patient safety: achieved through the development of an access system for emergency situations
- Transparency: ensured by rewarding patients in form of lower premiums.

4.8. MedRec

Among the new proposal to make possible to access data whenever and wherever they are needed, there is a blockchain framework called MedRec [43]. This framework is developed using the Ethereum blockchain and another kind of system called smart contract to make operations faster and automated. Indeed, through the implementation of these scripts, MedRec does not allow a direct

storage of data, but an encoding of pointers, which may be used to locate and authenticate all record locations in order to be accessed securely by patients. Moreover, MedRec defines three kinds of smart contract, which may belong to patients, providers, and other forms of users. These three mentioned types are:

1. Registrar Contract: it is used to map all participant IDs in order to be sure that only certified institutions are able to add new information into the blockchain. Moreover, each identity string is located at an address on the blockchain, which is assigned by a Summary Contract.
2. Patient-Provider Relationship Contract: it links two nodes in the system, where one of them is involved in the management and storage of all records of the other.
3. Summary Contract: it is useful to encode a list of Patient-Provider Relationship Contracts and to store each relationship as a "status" variable, which highlight when the relationship has been established and it has been approved by the patient.

All the mentioned possible relationship between different patient and provider contracts is shown in Figure 4.4.

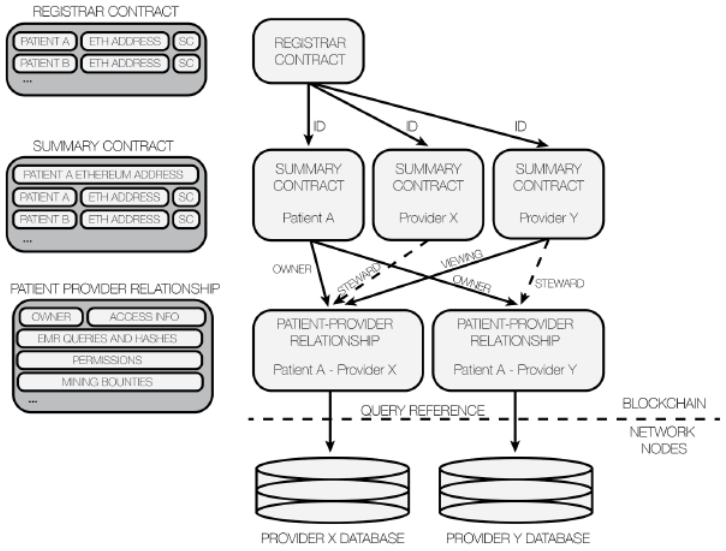


Figure 4.4 Three different kinds of Smart Contracts and their relationships

4.9. Akbar proposal

Developed in September 2021, the Akbar proposal deals with the implementation of the Ethereum blockchain for health records [44]. As shown in Figure 4.5, in the entire system workflow, there exists four main components, which are:

- Private Blockchain: it is built using four virtual servers and each of them is allowed to install an application called Geth to generate a blockchain node. Among the created nodes, only the

first one is used to mine, while the remaining entities are seen as ordinary nodes or hospitals ones.

- Smart Contract: it allows to manage rules in form of computer code and, since they are stored in the public blockchain, they cannot be tampered. Additionally, the nodes, which participate in this new framework, include both patients and hospitals. So, to test if the system is successful to share data, it is possible to analyse whether the patient data entered from one hospital can be accessed by other healthcare facilities. Meanwhile, the main function of smart contracts consists of the implementation of functions through which it is possible to add, modify or obtain data from patient or hospitals. Together with it, there is also an authentication system in order to ensure confidentiality and privacy aspects.
- Web Services: their implementation is made using the JavaScript programming language. They are used to send POST request like and API in order to facilitate interaction between users and system that has been created.

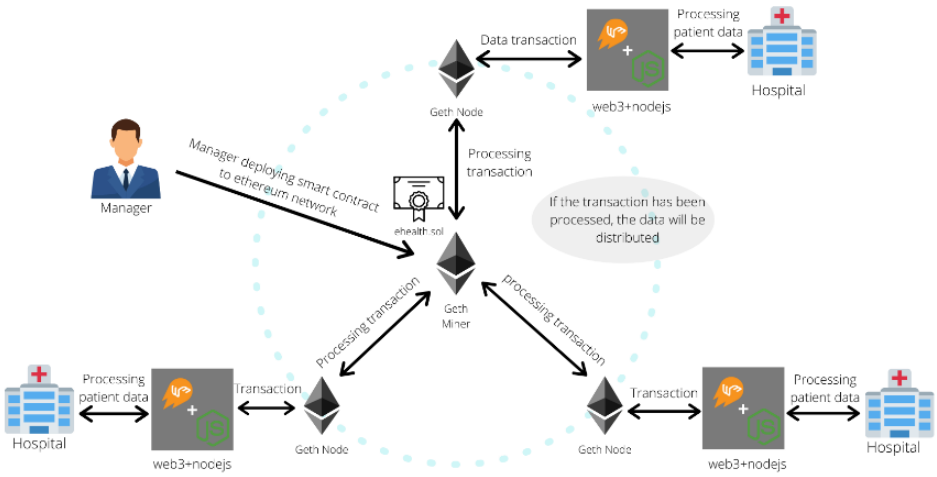


Figure 4.5 System Design

4.10. Sun proposal

Developed in 2020, the system framework proposed by Sun et al. [26] is made of five entities, which are shown in Figure 4.6, together with their interaction process. Here, each identity has its own specific rule, particularly there are:

- Patient: it is also the data user. Anytime a patient registers with an hospital, the server of the latter generates a certificate, which is sent to the patient and stored on the registration list of

the doctor. So, when a patient goes to the doctor, he gives to him the certificate in order to generate his personal medical data

- Doctor: it is the entity involved in the creation of medical information for the patient. Here, it is assumed to be honest and so, anytime a patient goes to the doctor, they discuss about an access policy to encrypt medical information. The ciphertext generated is made of two parts, the first one deals with the EHR, and it is stored in the IPFS, while the second part includes the keyword used between the two mentioned entities and so, it is stored inside the smart contract.
- Data Requester: it covers institutions such as scientific research, medical insurance companies or patient's families, which can obtain relevant records as long as their attributes meet the corresponding access policy.
- IPFS: it is the platform where the first part of the generated ciphertext, which deals with patient EHR, is stored. Moreover, it returns a hash value to the doctor, which indicates the corresponding file address.
- Blockchain Network: it is involved in the implementation of smart contracts, which allows to ensure the secure storage and sharing of EHR.

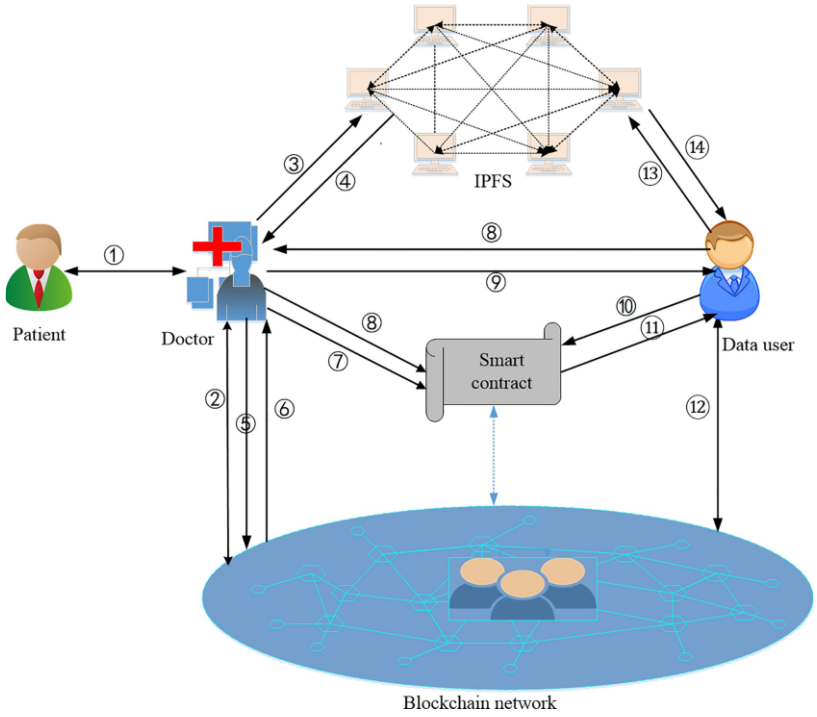


Figure 4.6 System Model

4.11. Trough proposal

Implemented in 2019, the Trough proposal [45] is a blockchain framework mainly aimed to achieve a GDPR-compliant personal data management platform through the development of a secure architecture, functions, and algorithms.

The entire workflow of the system is shown in Figure 4.7, where the three main participants are the Service Provider (SP), the Resource Server (RS), and the Blockchain Platform. Particularly, the operation flow is made of six steps, which are:

Step 1: the Server Provider performs an access request to the blockchain platform, which plays a role of a delegated authentication and authorization server.

Step 2: the authorized Service Provider receives an access token, which is a sort of proof of permission showing that a party is granted to access to a particular dataset.

Step 3: the access token is used by the Service Provider to request a desired data from the Resource Server.

Step 4: the Resource Server interacts with the Blockchain platform to validate the granted access by sending a token validation request.

Step 5: the Blockchain platform replies to the Resource Server with a Token Validity message

Step 6: the requested data are sent to the Server Provider.

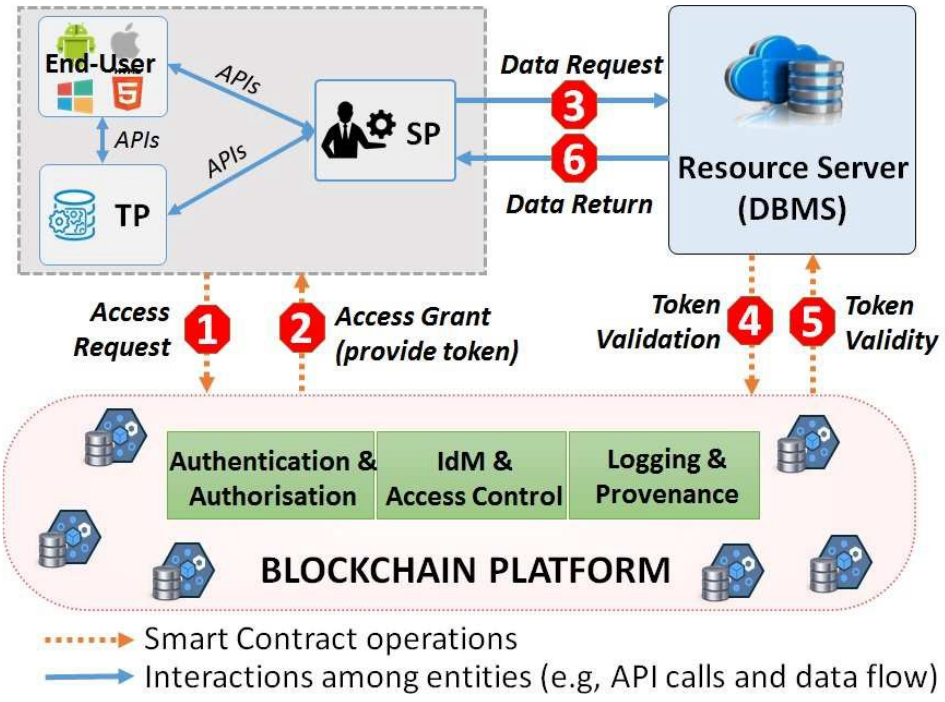


Figure 4.7 System Architecture

CHAPTHER 5

Ethical Analysis of Considered Blockchain Frameworks

This Chapter aims to provide a qualitative and a quantitative evaluation of ethics of blockchain frameworks considered in Chapter 3. All the answers given to controls of the constitutive ethical model, together with the corresponding reasons, are reported in the Appendix.

5.1. Qualitative Ethical Analysis of considered Blockchain-based Frameworks

Starting from the intersection between healthcare, blockchain and ethics, it could be interesting to focus on how the main characteristics of the proposed blockchain frameworks allow to follow the defined ethical pillars of Fairness, Accuracy, Privacy, Data Access, and Right to be Forgotten.

The **type of blockchain** shows to influence the ethical principles of *Fairness, Privacy* and *Data Access Control*. Specifically, the implementation of a private or permissioned blockchain could create contingencies in access opportunities to personal information. However, the property of *Fairness* could be considered satisfied also in case of permissioned or private blockchain assuming that, once nodes are verified, they are subjected to equal access opportunities. For what concerns *Data Access Control* and *Privacy*, these ethical principles result to be more satisfied in case of a private or permissioned blockchain implementation, since nodes are always verified, and the data owner can determine who can visualize its own personal information.

The implemented **consensus mechanism** is important to highlight possible changes in the accomplishment of the *Fairness* principle. Indeed, if the chosen consensus mechanism is the Practical Byzantine Fault Tolerance (PBFT) or the Proof of Work (PoW), the mentioned ethical property can be considered satisfied. This is because, for example in the case of PBFT, the right to mine is given not only to a particular set of nodes, but every user has the same possibility of adding blocks. On the other hand, if the type of implemented consensus mechanism is the Proof of Authority (PoA), *Fairness* results to be compromised since this choice gives rise to the identification of a limited number of participants which have the power to validate transactions.

The choices of **storage mechanisms**, **encryption of data**, together with the presence of other forms of **decentralized storage**, such as the Inter-Planetary File System (IPFS), may determine the

accomplishment of the *Right to be Forgotten* principle. Indeed, if a data is stored off chain, such as in a database or in other decentralized storage systems, the GDPR requirement of giving the right to the data owner to erase their information whenever they want results to be fully satisfied. Nevertheless, even if data are stored on-chain, the possibility to encrypt them guarantee the possibility to delete information by throwing away the secret key.

The implementation of **anonymization techniques**, together with **authentication systems** and **data access controls** are useful to preserve *Privacy* of users and patients. Indeed, through these characteristics, there is the possibility to know who participate to the network and, additionally, the selection of the portion of data that an entity can visualize is allowed. However, without any other specifications, the mentioned possibility of selecting who and how data can be visualized appears to be in contrast with the *Fairness* principle, since, in this case, the equity in access opportunities results to be compromised.

Finally, forms of **on-chain computations**, such as the presence of smart contracts, enhance the accuracy level of data processing and management since they represent a way to perform any type of computation being sure that the code cannot be damaged or modified due to the immutable nature of blockchain.

Based on the mentioned implementation aspects, the core technology of each medical blockchain-based model is respectively synthesized in Table III.

Table III List of Core Technology of the Analysed Medical Blockchain-based Models

Healthcare Blockchain-based Model	Type of Blockchain	Consensus Mechanism	Storage of Data	Encryption of Stored Data	Anonymization	On-Chain Computations (Smart Contract)	Authentication Mechanism	Data Access Control	IPFS
DiTrust	Permissioned	Not Specified	Off-Chain	NO	NO	YES	Mutual Authentication	YES	YES
CP-DBHCA	Private	Not Specified	On-Chain	YES	NO	YES	Multi-Factor	YES	NO
HealthBlock	Permissioned	PBFT	Off-Chain	NO	NO	YES	Biometric	YES	NO
Mexchange	Permissioned	PoW	Off-Chain	YES	YES	YES	Two-Factor	YES	NO
Mukesh proposal	Permissioned	PBFT	On-Chain	YES	NO	YES	Multi-Factor	YES	NO
hOCBS	Permissioned	PoA	Off-Chain	NO	YES	YES	Two-Factor	YES	NO
MedicalChain	Private	Not Specified	Off-Chain	YES	NO	YES	Biometric	YES	YES
MedRec	Permissioned	PoW	On-Chain	YES	NO	YES	Two-Factor	YES	NO
Akbar proposal	Private	Not Specified	On-Chain	YES	NO	YES	Multi-Factor	YES	NO
Sun proposal	Public	Not Specified	Off-Chain	YES	YES	YES	Two-Factor	YES	NO
Trough proposal	Permissioned	PBFT	On-Chain	YES	YES	YES	Access Token	YES	NO

According to the technical aspects of each blockchain-based framework highlighted in Table III, Table IV shows, for each model, which are the fulfilled ethical principles. Specifically, the reason why some ethical features result not to be satisfied in some of the proposed blockchain framework can be explained as follows:

- **CP-DBHCA:** the property of *Fairness* results not to be satisfied because, through the implementation of a private blockchain, the model shows to be vulnerable to attacks such as the privilege based one.
- **HealthBlock:** the *Accuracy* of data is not fully accomplished because the system gives the possibility to be sure about the trustworthy of data only once they are introduced inside the blockchain and does not allow to have any evidence about the veracity of the original data.
- **hOCBS**: due to the usage of Proof of Authority as a consensus mechanism, the system becomes in contrast with the ethic requirement of *Fairness.*
- **MedicalChain:** due to the user capability to provide different levels of access and to design who can query and write data on the blockchain without giving any other specifications, the *Fairness* property becomes compromised.
- **MedRec**: the original data cannot be verified by any type of technique, so the **Accuracy** principle results not to be fully satisfied, since it is guaranteed only once data are inserted in the blockchain.
- **Akbar proposal**: the private blockchain component of the framework leads to a loss of *Fairness* since the right to mine is given only to the first created node, while the others are used as ordinary or hospital nodes.

Table IV Qualitative Ethical Analysis of the proposed Blockchain-based frameworks

Healthcare Chain based Model	**Ethics Features**				
	Fairness	*Privacy*	*Accuracy*	*Right to be Forgotten*	*Data Access*
DiTrust	🟢	🟢	🟢	🟢	🟢
CP-DBHCA	🔴	🟢	🟢	🟢	🟢
HealthBlock	🟢	🟢	🟡	🟢	🟢
Mexchange	🟢	🟢	🟢	🟢	🟢
Mukesh proposal	🟢	🟢	🟢	🟢	🟢
hOCBS	🔴	🟢	🟢	🟢	🟢
MedicalChain	🔴	🟢	🟢	🟢	🟢
MedRec	🟢	🟢	🟡	🟢	🟢
Akbar proposal	🔴	🟢	🟢	🟢	🟢
Sun proposal	🟢	🟢	🟢	🟢	🟢
Trough proposal	🟢	🟢	🟢	🟢	🟢

5.2. Results of the Constitutive Ethical Analysis

The ethical evaluation is obtained by analysing scores associated to each ethical principle and computing the average of them, weighted according to the number of implemented controls. Particularly, starting from all information of each blockchain framework present in the literature, the correct answer to each control has been selected. On this regard, a summary table (Table V), reporting all the final ethical scores of the analysed blockchain models, is built and the colour choice is done according to the following thresholds:

- $0 \leq \text{score} < 6 \rightarrow$ red;
- $6 \leq \text{score} < 8 \rightarrow$ yellow;
- $8 \leq \text{score} \leq 10 \rightarrow$ green.

Table V Summary Table of the Constitutive Ethics Model's Outputs

Blockchain	**Scores**					**Final Ethical Score**
	Fairness	*Data Governance and Privacy*	*Accuracy*	*Right to be Forgotten*	*Responsibility*	
DiTrust	8	8.75	10	10	10	9.06
CP-DBHCA	6	8.75	10	5	10	7.81
HealthBlock	8	8.75	5	10	10	8.44
Mexchange	7	8.75	10	10	8.33	8.44
Mukesh proposal	6	8.75	10	10	8.33	8.13
hOCBS	6	8.75	10	10	8.33	8.13
MedicalChain	6	8.75	10	5	10	7.81
MedRec	8	8.75	5	10	10	8.44
Akbar proposal	6	8.75	10	5	10	7.81
Sun proposal	8	8.75	10	10	6.67	8.44
Trough proposal	8	8.75	10	10	10	9.06

Based on Table V, it is possible to assess which blockchain frameworks can be considered the best ones in achieving the maximum level of adherence to the constructed ethical evaluation model. On this regard, the higher level of ethical performance is achieved by **DiTrust Chain** and the **Trough proposal**, which obtain a final ethical score equal to 9.06. Particularly, for both blockchain frameworks, the most accomplished ethical pillars are *Accuracy, Right to be forgotten* and *Responsibility*.

On the other hand, the yellow-coloured boxes of the last column of Table IV represent those blockchain frameworks for which the model gives the worst final output. Specifically, they are **CP-DBHCA, Medical Chain** and the **Akbar proposal**, which obtain an overall evaluation equal to 7.81. Focusing on which ethical principles result to be difficult to implement, it is possible to observe that in all of them a non-sufficient score is given to the property of *Right to be forgotten* and a slightly sufficient evaluation is given to the *Fairness* feature.

Finally, looking at the best and the worst accomplished ethical principles, it is possible to highlight that *Data Governance and Privacy* is achieved with a high score for all the analysed blockchain frameworks, while the *Fairness* property results to be the hardest ethical feature to respect, since, in most of the cases, it is represented with a score equal to 6.

5.3. Comparison between the Qualitative and Quantitative Ethical Evaluations

The aim of the constitutive ethics model is to achieve an evaluation of the analysed frameworks considering the most important pillars of ethics. Additionally, the comparison between the qualitative and the quantitative analysis enables to assess how the implemented model allows to highlight which aspects and which blockchain frameworks achieve the best and the worst ethical scores. On this regard, Figure 5.1 shows the Tables IV and V one close to the other, in order to have a visual reference of the performed comparison.

a)

Healthcare Chain based Model	Ethics Features				
	Fairness	*Privacy*	*Accuracy*	*Right to be Forgotten*	*Data Access*
DiTrust	●	●	●	●	●
CP-DBHCA	●	●	●	●	●
HealthBlock	●	●	●	●	●
Mexchange	●	●	●	●	●
Mukesh proposal	●	●	●	●	●
hOCBS	●	●	●	●	●
MedicalChain	●	●	●	●	●
MedRec	●	●	●	●	●
Akbar proposal	●	●	●	●	●
Sun proposal	●	●	●	●	●
Trough proposal	●	●	●	●	●

b)

Blockchain	Scores					Final Ethical Score
	Fairness	*Data Governance and Privacy*	*Accuracy*	*Right to be Forgotten*	*Responsibility*	
DiTrust	8	8.75	10	10	10	9.06
CP-DBHCA	6	8.75	10	5	10	7.81
HealthBlock	8	8.75	5	10	10	8.44
Mexchange	7	8.75	10	10	8.33	8.44
Mukesh proposal	6	8.75	10	10	8.33	8.13
hOCBS	6	8.75	10	10	8.33	8.13
MedicalChain	6	8.75	10	5	10	7.81
MedRec	8	8.75	5	10	10	8.44
Akbar proposal	6	8.75	10	5	10	7.81
Sun proposal	8	8.75	10	10	6.67	8.44
Trough proposal	8	8.75	10	10	10	9.06

Figure 5.1 a) Summary table of the qualitative ethical analysis of the considered blockchain frameworks; b) Summary table of the quantitative ethical analysis of the considered blockchain frameworks

Considering **the best blockchain frameworks** given by the qualitative analysis, which result to be DiTrust Chain, Mexchange, Mukesh proposal, Sun proposal and Trough proposal, the quantitative model highlights that *DiTrust Chain* and *Trough proposal* achieve the best final ethical score equal to 9.06. Looking at the common aspects of these two blockchain frameworks, it is possible to observe that the zero-state problem is solved through the request for information about the way in which data have been processed. Particularly, for DiTrust chain, the first layer comprises of sensors and actuators and has the function of querying location, temperature, blood pressure, weight, motion, vibration, humidity, etc., while for the Trough proposal, data activities should be logged in the distributed ledger containing information about 'who', 'why', 'when', 'what' and 'how' personal data are analysed. Additionally, another aspect that characterizes both frameworks is the implementation of

a permissioned blockchain, which plays an important role in authenticating and authorizing nodes enjoying in the network and allows access opportunities not to be influenced by any form of contingencies. Finally, the storage mechanism of data is implemented off-chain and in an encrypted way, giving the possibility to modify or delete information whenever it is needed.

For what concern **the worst blockchain frameworks** given by the qualitative analysis, which result to be CP-DBHCA, hOCBS, Medical Chain and the Akbar proposal, the quantitative model highlights that *CP-DBHCA, Medical Chain* and the *Akbar proposal* achieve the worst final ethical score equal to 7.81. Looking at the common aspects of these frameworks, it is possible to assess that they are characterized by the implementation of a private blockchain. Particularly, in case of CPDBHCA and Medical Chain, the private distributed ledger gives to the user the capability to provide different levels of access and to design who can query and write data, while, in case of Akbar proposal, the implemented blockchain leads to a network where only the first node has the right to mine. Moreover, the storage mechanism concerns with the possibility to archive data directly on-chain. Related to this characteristic, even if in the qualitative analysis the ethical property of "Right to be forgotten" has been represented with a green dot, the final output for this principle in the quantitative model is completely different. It is because, in the qualitative examination, it is considered only the possibility to throw away the key once the owner wants to erase his data, while, in the quantitative model it is taken into consideration also the immutable nature of the blockchain, which leads to the impossibility to modify data once they are inserted directly inside the blockchain.

From the comparison between the qualitative and quantitative model, it is possible to notice that, in case of Mukesh proposal the final output of the conducted analyses is slightly different. On this regard, in the qualitative evaluation, the proposed blockchain framework gives, as result, the accomplishment of all ethical pillars, while, through the quantitative model, the final score is lower with respect to many other analysed systems. A possible reason behind this difference may be due to the specificity of the selected controls for the implementation of the evaluation model. Indeed, the set of controls is not only focused in guaranteeing the absence of biases, but also in determining the possibility to provide some compensatory tools, if needed, in order to not make access opportunities to be influenced by any form of contingencies. So, while in the qualitative analysis the accomplishment of the fairness property is evaluated only considering discriminations between categories, such as gender or race, in the quantitative model, the presence of controls gives the possibility to extend the ethical analysis of fairness into a wider range of aspects related to this property.

All ethical scores of the analysed blockchain frameworks are shown through a histogram in Figure 5.2.

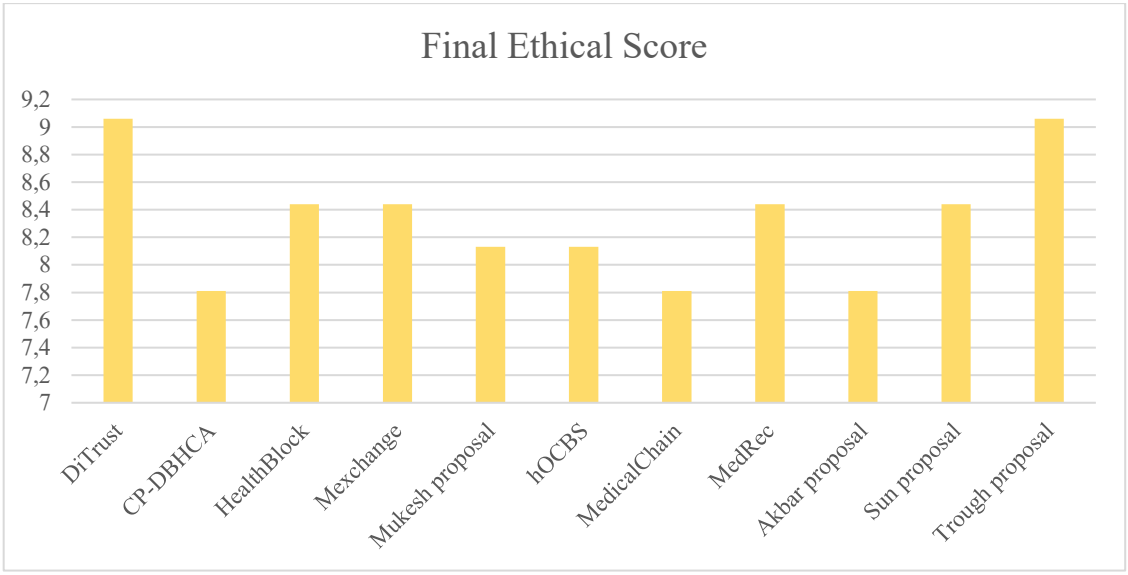


Figure 5.2 Ethical scores of the analysed blockchain frameworks given by the Constitutive Ethical Model

Considering not only the differences between the qualitative and quantitative evaluations of different blockchain frameworks, but also the variability in complying with all the ethical principles, it is possible to observe that some of them, which have been considered satisfied in the qualitative analysis result not to be respected in the quantitative one. On this regard, from the qualitative evaluation, the ethical pillars of *Privacy, Right to be forgotten* and *Data Access* are represented with all green dots. On the other hand, in the quantitative ethical model, the second ethical principle results to be not completely satisfied and the features of *Privacy* and *Data Access* are putted together as a unique characteristic, due to the difficulty to create separated and independent controls for these two principles. Looking in detail to these three ethical pillars, the reason why Privacy is fully satisfied both in the qualitative and quantitative analyses is because every blockchain framework is built starting from the concept of privacy preservation. Moreover, the accomplishment of Data Governance property is linked to the concept of patient centric control over their data, which means that there is always a system that avoid collecting or running data if no consent is given. On the other hand, as specified above, the *Right to be forgotten* is not fully respected considering the immutable nature of blockchain and the presence of some analysed frameworks which provide an on-chain storage of processed data.

Finally, for what concerns the hardest ethical principle to respect, the output of both the qualitative and quantitative analyses give as result the Fairness property. Indeed, even if, differently from the qualitative analysis, in the quantitative one the used colours are green and yellow, this ethical principle is characterized by the lowest score in many of the analysed blockchain frameworks. The reason why, as shown in Figure 5.3, many blockchain systems are unable to fully satisfy this ethical principle can be different according to the type of implemented distributed ledger. Specifically, the cause can be that sensitive data are rarely used to evaluate the necessity to require some compensatory tools, or that the implementation of a private blockchain structure makes the access opportunities to

be influenced by some forms of contingencies, or that the patient has a full control over their data which could lead to the possibility to select which portion of personal information another user can visualize and, more generally, who can analyse data and who cannot.

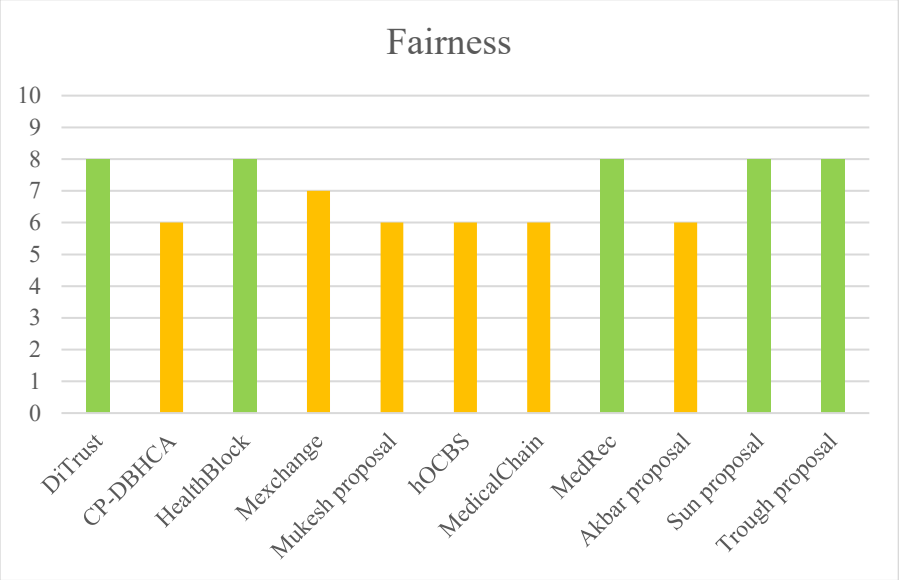


Figure 5. 3 Fairness Property scores of the analysed blockchain frameworks

Conclusion

Nowadays, with medical advances and the increased dynamics of clinical systems, the management of patient's health record is becoming one of the most relevant challenges faced by healthcare providers. So, starting from this concept, the presented study stems from the idea that providing an innovative ethical evaluation model, which is able to furnish a score to the ethical behaviour of any analysed system, could help organizations to have a more precise and objective evaluation of the ways in which data are processed and shared, instead of a qualitative and subjective assessment.

After describing the most recent blockchain frameworks proposed in the literature, which are implemented on the basis of privacy preservation, and defining the general concept of ethics, a qualitative and a quantitative overview has been provided, identifying the main ethical challenges, and evaluating if they are respected or not. The considered ethical pillars, which have been used for these two types of analyses are Fairness, Privacy, Accuracy, Data Governance and Responsibility. Moreover, in this work, ethics has been defined in terms of Constitutive and Circumstantial, which indicate, respectively, the level of adherence of any system to the ethical evaluation framework, and the combination between the constitutive ethics and the technical complexity of the organization. From these definitions, two different models have been implemented, where, for each identified category of the analyses, a set of sub controls has been constructed. Finally, having both the outputs of the qualitative analysis and the constitutive ethics model, a comparison between them has been performed in order to assess similarities and differences of the final ethical evaluations, and how the quantitative analysis could improve the qualitative one.

Although recently blockchain-based medical systems are a hot topic, according to the latest studies, there is no quantitative ethical analysis related to their use. This study firstly offers an implementation of an ethical evaluation framework and secondly performs a quantitative analysis that aims to highlight which characteristics of these systems could improve the ethical score and which ethical features result to be the simplest and the hardest ones to follow. On this regard, the highest final ethical score has been provided by those frameworks having a permissioned blockchain and allowing an off-chain storage and encryption of processed data, contrary to the implementation of private blockchain with an on-chain storage mechanism, which obtain the lowest ethical evaluation score. Additionally, the fully realized ethical aspects, defined by the constitutive ethics model, are Privacy

and Data Governance. It is because the analysed models have the objective of preserving the privacy of citizens and every blockchain framework provides a patient centric control over their data. On the other hand, as already observed from the qualitative analysis, the Fairness property is the hardest one to satisfy, since it includes not only the absence of biases, but also the absence of contingencies influencing access opportunities and the possibility to provide compensatory tools whenever they are needed.

To conclude, this study could represent a starting point for further research, since it gives a first ethical evaluation model which is able to quantify the level of ethics of any organization in processing and sharing their data. One limitation of this work is that it focuses its analysis only on blockchain-based systems, analysing a limited set of them. Additionally, for some ethical pillars, the number of implemented controls results to be too low to have a precise quantitative information about their accomplishment. Further studies could enlarge the set of analysed blockchain frameworks and implement more controls for each ethical pillar, in order to achieve a more precise evaluation. Moreover, the implemented constitutive ethics model could be applied also to other types of organizations and to other types of implemented systems for data management and storage, such as databases.

Bibliography

[1] Asare, Patience, Edward W. Ansah, and Francis Sambah. "Ethics in healthcare: Knowledge, attitude and practices of nurses in the Cape Coast Metropolis of Ghana." Plos one 17.2 (2022): e0263557.

[2] Sharif, Monica M., and Farshad Ghodoosi. "The ethics of blockchain in organizations." Journal of Business Ethics (2022): 1-17.

[3] Brey, Philip AE. "Anticipating ethical issues in emerging IT." Ethics and Information Technology 14.4 (2012): 305-317.

[4] Palm, Elin, and Sven Ove Hansson. "The case for ethical technology assessment (eTA)." Technological forecasting and social change 73.5 (2006): 543-558.

[5] Stahl, Bernd Carsten, et al. "Identifying the ethics of emerging information and communication technologies: An essay on issues, concepts and method." International Journal of Technoethics (IJT) 1.4 (2010): 20-38.

[6] Nehme, Esther, et al. "Converged AI, IoT, and blockchain technologies: a conceptual ethics framework." AI and Ethics (2021): 1-15.

[7] Srivastava, Vandana, Tripti Mahara, and Pooja Yadav. "An analysis of the ethical challenges of blockchain-enabled E-healthcare applications in 6G networks." International Journal of Cognitive Computing in Engineering 2 (2021): 171-179.

[8] Tsamados, Andreas, et al. "The ethics of algorithms: key problems and solutions." AI & SOCIETY 37.1 (2022): 215-230.

[9] Stefano Armenia et al. Controlli Essenziali di Cybersecurity. Research Center of Cyber Intelligence and Information Security Sapienza Università di Roma (2017)

[10] Dipartimento di Ingegneria dell'informazione (DII) UNIVPM Cyber Risk Assessment Models and Algorithms (CybeRAMA) https://cyberama.dii.univpm.it/ (2020)

[11] https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/

[12] Floridi, L. Establishing the rules for building trustworthy AI. Nat Mach Intell 1, 261–262 (2019). https://doi.org/10.1038/s42256-019-0055-y

[13] Giovanola, Benedetta, and Simona Tiribelli. "Beyond bias and discrimination: redefining the AI ethics principle of fairness in healthcare machine-learning algorithms." AI & society (2022): 1-15.

[14] Abdu, Nail Adeeb Ali, and Zhaoshun Wang. "Blockchain for Healthcare Sector-Analytical Review." IOP Conference Series: Materials Science and Engineering. Vol. 1110. No. 1. IOP Publishing, 2021

[15] Kirchschläger, Peter. (2021). Ethics of Blockchain Technology. 10.5771/9783748924012-185.

[16] Genelot D. (2014) Responsabilità Etica nell'azione entro una complessità

[17] "Smuha, Nathalie A. "The EU approach to ethics guidelines for trustworthy artificial intelligence." Computer Law Review International 20.4 (2019): 97-106.

[18] "https://www.zerounoweb.it/techtarget/searchdatacenter/sicurezza-wireless-le-differenze-tra-la-crittografia-wep-wpa-e-wpa2/

[19] Prakash, Ambuj, and Umesh Kumar. "Authentication protocols and techniques: a survey." Int. J. Comput. Sci. Eng 6.6 (2018): 1014-1020.

[20] Yugha, R., and S. Chithra. "A survey on technologies and security protocols: Reference for future generation IoT." Journal of Network and Computer Applications 169 (2020): 102763.

[21] Olteanu, Alexandra, et al. "Social data: Biases, methodological pitfalls, and ethical boundaries." Frontiers in Big Data 2 (2019): 13.

[22] Soni, Mukesh, and Dileep Kumar Singh. "Blockchain implementation for privacy preserving and securing the healthcare data." 2021 10th ieee international conference on communication systems and network technologies (CSNT). IEEE, 2021.

[23] Al Omar, Abdullah, et al. "Privacy-friendly platform for healthcare data in cloud based on blockchain environment." Future generation computer systems 95 (2019): 511-521.

[24] Dwivedi, Ashutosh Dhar, et al. "A decentralized privacy-preserving healthcare blockchain for IoT." Sensors 19.2 (2019): 326.

[25] Abou-Nassar, Eman M., et al. "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems." IEEE Access 8 (2020): 111223-111238.

[26] Sun, Jin, et al. "A blockchain-based framework for electronic medical records sharing with fine-grained access control." Plos one 15.10 (2020): e0239946

[27] Ismail, Leila, Huned Materwala, and Alain Hennebelle. "A scoping review of integrated blockchain-cloud (BcC) architecture for healthcare: applications, challenges and solutions." Sensors 21.11 (2021): 3753.

[28] Raikwar, Mayank, Danilo Gligoroski, and Katina Kralevska. "SoK of used cryptography in blockchain." IEEE Access 7 (2019): 148550-148575.

[29] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). Ieee, 2017.

[30] Gervais, Arthur, et al. "On the security and performance of proof of work blockchains." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.

[31] Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." Data privacy management, cryptocurrencies and blockchain technology. Springer, Cham, 2017. 297-315.

[32] Karantias, Kostis, Aggelos Kiayias, and Dionysis Zindros. "Proof-of-burn." International conference on financial cryptography and data security. Springer, Cham, 2020.

[33] Yu, Ge, Bin Wu, and Xinxin Niu. "Improved blockchain consensus mechanism based on PBFT algorithm." 2020 2nd International Conference on Advances in Computer Technology, Information Science and Communications (CTISC). IEEE, 2020.

[34] Ahmed-Rengers, Mansoor, and Kari Kostiainen. "Don't Mine, Wait in Line: Fair and Efficient Blockchain Consensus with Robust Round Robin." arXiv preprint arXiv:1804.07391 (2018).

[35] Mohammed, Alaa Hamid, Alaa Amjed Abdulateef, and Ihsan Amjad Abdulateef. "Hyperledger, Ethereum and blockchain technology: A short overview." 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE

[36] H. Kenneth, "Ethereum account", Medium: Coinmonks, 7 May 2018. [Online]. Available: https://medium.com/coinmonks/ethereum-account-212feb9c4154.

[37] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[38] Ghayvat, Hemant, et al. "CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications." IEEE Journal of Biomedical and Health Informatics (2021).

[39] Zaabar, Bessem, et al. "HealthBlock: A secure blockchain-based healthcare data management system." Computer Networks 200 (2021): 108500.

[40] Lee, Deoksang, and Minseok Song. "MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address." IEEE Access 9 (2021): 158122-158139.

[41] Miyachi, Ken, and Tim K. Mackey. "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design." Information Processing & Management 58.3 (2021): 102535.

[42] Medicalchain, "Whitepaper", 2018. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

[43] MedRec, "Whitepaper", 2018. [Online]. Available: https://medrec.com/ medrec_technical_documentation.pdf

[44] Akbar, Irfan Maulana, Adhitya Bhawiyuga, and Reza Siregar. "An Ethereum Blockchain Based Electronic Health Record System for Inter-Hospital Secure Data Sharing." 6th International Conference on Sustainable Information Engineering and Technology 2021. 2021

[45] Truong, Nguyen Binh, et al. "Gdpr-compliant personal data management: A blockchain-based solution." IEEE Transactions on Information Forensics and Security 15 (2019): 1746-1761.

Appendix

1) DITRUST

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: the first layer comprises of sensors and actuators required for different functions such as querying location, temperature, blood pressure, weight, motion, vibration, humidity, etc.

- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  YES: the first layer is dedicated for collecting and processing information as well as making necessary changes to such data. This is the application layer that facilitates trust between members on the IoT network

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: there is a system that avoid collecting or run a set of data if no consent has been given

- *Evaluation of credentials of employees every time a new access is performed*

  YES: the privacy or confidentiality of the system is realised using Health edge through Ripple chain based on validated nodes.

- *Citizen's level of control over their data access and privacy*

  HIGH: transactions are stored in Ripple chain, thus making it possible to modify or access the data ONLY for nodes related to this transaction, which guarantees date privacy for patients.

- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: the authentication system implemented is the mutual one, so, an end-to-end authentication request is needed to access to the system.

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES*:* because of the presence of a mutual authentication system, which allows parties to validate credential to each other. Additionally, the signatures generated using the elliptic curve signature algorithm ensure the trustworthiness and seamless of data integration between members.

- *The distribution of access opportunities is not influenced by any form of contingencies*

  YES: Unlike private Blockchain, in Ripple Blockchain, permission is not confined to one organisation or any specified member. Here, each group has a primary member that detects its group and provides accessibility to every object that has permission.

- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  NO: there is not this type of mechanism in the proposed framework

- *Level of heterogeneity of the sources of the data used and analysed*

  HIGH: The heterogeneity of electronic health records (EHRs) in healthcare-IoT systems (i.e. IoHT) comes from medical records collected across various service providers, and complexity

  in accessing as well as reusing such data makes it a vital challenge for realising efficient IoHT

- *Type of classification method used*

  CALIBRATION: In some instances, out-of-hospital medical care is provided to the patient by referring them to specialists (i.e. Doctors). In the DIT framework, in emergency or special patient cases, EMS communicates with hospitals (via notification messages), for example, to reserve operation theatres. Otherwise, EMS communicates with Specialist by sending patients' case report to prescribe a suitable treatment.

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  YES: use of the health-edge for data storage, which has not the immutable property of the blockchain and so, it becomes possible to modify and delete any personal data.

- *Use of approved cryptographic mechanisms to protect data stored*

  YES: data are stored in the health-edge in an encrypted way

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  HIGH: the reliability between members is assessed using hashing and a signed exchanged message. The signatures generated using the elliptic curve signature algorithm ensure the trustworthiness and seamless of data integration between members.

- *Type of responsibility implemented*

  MONADIC: due to the mutual authentication, it considers the general definition of responsibility without giving any other forms of specification

- *Volume of responsibility defined*

  SOLE RESPONSIBILITY: due to the mutual authentication, the owner of a decision can be easily identified.

2) CPDBHCA

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: one of the main novelties of the system is to consider 130 attributes such as patient ID, credentials, and contact information. We have installed BC adapters with required touchpoints at various healthcare facility locations to form patient profiling records.

- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  N/A: through the storage of the difference between the received and forwarded timestamps, it is possible to face Replay attacks, however, there is not the interacted surface for an evaluation performed by the owner or clinicians

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: The proposed scheme presents two frameworks. In the first framework, named as HCA-ECC, the HCA authentication and authorization is handled via a secure session establishment through ECC between the cloud and the application layer. Once keys are established, secure EHR access and sharing are handled through BC.

- *Evaluation of credentials of employees every time a new access is performed*

YES: for the access control, the integration of Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) is computed, generating a scheme called HCA-RSAE. Here, the generation of secure key pairs is performed to allow communication between authorized entities.

- *Citizen's level of control over their data access and privacy*

  MEDIUM: Accessibility and authorization – Smart contracts are used to check if an individual has the right to access the data. This covers the confidentiality portion a bit as the only intended user can access the data. Moreover, once keys for communication are established, secure EHR access and sharing are handled through BC and not by the patient.
- *Level of security of the authentication system used every time a new access is performed*

  HIGH: entities credentials are made of HealthID, Patient Name, Patient Picture, Patient Address, Biometric

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES*:* through the use of a key pair generation, any communication must be adequately justified towards all the other parts involved.
- *The distribution of access opportunities is not influenced by any form of contingencies*

  NO: to access data it is necessary to generate a wallet address, where, among public available EHR information there are Health Tags, Lifestyle indicators, Clinical history, and Age
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  NO: there is not this type of mechanism in the proposed framework
- *Level of heterogeneity of the sources of the data used and analysed*

  HIGH: In smart healthcare ecosystems, embedded internet-of-things (IoT) based body wearables generate enormous healthcare big-data (HBD). The generated data is heterogeneous, fragmented, and diverse, and is stored at multiple locations
- *Type of classification method used*

  ANTI-CLASSIFICATION: it is not explicitly said that sensitive data stored in the wallet are used in any decision-making process

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  NO: data are encrypted and stored directly on-chain. However, the right to be forgotten is guaranteed by throwing away the key once data need to be erased.
- *Use of approved cryptographic mechanisms to protect data stored*

  YES: data are stored in an encrypted way

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  HIGH: the generation of session keys useful for access data and performed transactions starts with the generation of walled addresses, which contains any information useful for identify an individual
- *Type of responsibility implemented*

  DYADIC: due to the wallet addresses generation, it is possible to underline the responsibility of an individual for any specific action.
- *Volume of responsibility defined*

  SOLE RESPONSIBILITY: due to the wallet addresses generation, the owner of a decision can be easily identified.

3) HealthBlock

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: use two blockchain channels: medical devices blockchain channel and remote consultation blockchain channel. More precisely, the devices blockchain channel is used by patients and physicians to handle wearable health devices details, assignment, and status. This channel also saves related IoT gateway details.
- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  NO: The sixth layer is the Users Layer which consists of patients, physicians, pharmacists and laboratory technicians who interact with the HealthBlock and benefit from its functionalities, however there is not any indication about the possibility to evaluate the correctness of information before entering data in the blockchain

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: the consultation blockchain channel is used by patients, physicians, pharmacists and laboratory technicians to control access to patient's healthcare data, to deliver requested vital signs and to share healthcare data with concerned participants.

- *Evaluation of credentials of employees every time a new access is performed*

  YES: To effectively deploy the proposed architecture, a permissioned blockchain is used because it maintains the access control to only specific participants which will secure the data access.

- *Citizen's level of control over their data access and privacy*

  HIGH: we have used a permissioned consortium blockchain in order to allow only specific

  participants to benefit from the proposed healthcare services. Also, we have implemented access control policies for those participants. In essence, Access control permission rules precise who is allowed and to which sensitive data has access. Besides, We have adopted a patient centric approach system where the patient has full control to grant or deny access permissions to the authorized stakeholders.

- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: In the proposed system, the participants are restricted to be patients, physicians, pharmacists, and laboratory technicians. So, they are previously identified through biometric or OTP modalities

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES: the application layer works on a peer-to-peer network and communicates to a deployed smart contract through Application Programming Interfaces (APIs).

- *The distribution of access opportunities is not influenced by any form of contingencies*

  NO: In the proposed system, the participants are restricted to be patients, physicians, pharmacists, and laboratory technicians.

- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

YES: In the proposed system, only the permissioned or authenticated participants can have access to the electronic health record of a specific patient for a particular session. Since we have adopted a patient centric approach in which the patient manages his private data, the
confidential nature of health data is preserved.

- *Level of heterogeneity of the sources of the data used and analysed*
  HIGH: since data come from wearable devices the level of heterogeneity of them will be very high
- *Type of classification method used*
  ANTI-CLASSIFICATION: patient centric approach in which the patient manages his private data, they cannot be used for classification purposes.

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*
  YES: The third layer is the off-chain database one, which produce hash values of data and sends them to the blockchain database.
- *Use of approved cryptographic mechanisms to protect data stored*
  YES: The vital signs data are encrypted and stored in a decentralized database

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*
  HIGH: As the proposed blockchain participants are pre-registered and identified, therefore every action such as transaction submission, network configuration modifications are all recorded in the blockchain ledger state database.
- *Type of responsibility implemented*
  DYADIC: any transaction or modifications will be recorded in the blockchain ledger database.
- *Volume of responsibility defined*
  SOLE: the blockchain is a permissioned one and participant must be pre-registered and identified.

4) Mexchange

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

YES: data are given by hospital, and they are taken from their database. So, the receiving information will be full of description

- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  YES: the Presentation layer enable to have the user interface for interacting directly with other endpoints.

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: the entire workflow of the system concerns with the four main steps and, among them, there is the access request performed by a user to the patient
- *Evaluation of credentials of employees every time a new access is performed*

  YES: thanks to the use of permissioned blockchain
- *Citizen's level of control over their data access and privacy*

  HIGH: the entire workflow of the system concerns with the four main steps and, among them, there is the access request performed by a user to the patient
- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: A user generates private key, public key, and address to access to the system

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES: The scheme of this model is made up of four players, which are the Certificate Authority (it authenticates new participants and records them in the blockchain), Hospitals (they manage health information in databases), Patients (they grant access to the requestors and exchange health information), and Requestors (they ask patients for access and request health information from hospitals)
- *The distribution of access opportunities is not influenced by any form of contingencies*

  NO: since the system works with a private blockchain only authorized users can access to data in a manner defined by the patient.
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  N/A: there is no specification about the type of sensitive data acquired and if they are used or not to require compensatory tools.

- *Level of heterogeneity of the sources of the data used and analysed*

  MEDIUM: data derive from hospitals databases, however, MEXchange cannot handle large volumes of transactions quickly.
- *Type of classification method used*

  ANTI-CLASSIFICATION: protected categories are not explicitly used in the decision-making process

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  YES: due to the off-chain data storage in an encrypted way, it is possible to delete any kind of information by making computation on the modifiable database.
- *Use of approved cryptographic mechanisms to protect data stored*

  YES: due to the off-chain data storage in an encrypted way, it is possible to delete any kind of information by making computation on the modifiable database.

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  MEDIUM: due to the ring signature implementation
- *Type of responsibility implemented*

  MONADIC: due to the obscuration of the sender and the receiver it is possible only to determine the general concept of responsibility without giving any other specification
- *Volume of responsibility defined*

  SHARED: due to the implementation of the ring signature

5) Mukesh proposal

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: since medical data are delivered by hospitals
- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  YES: To verify the medical data immediately and authenticates the zero-knowledge evidence without involving the third-party, smart contract is required.

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: patient can own and share his personal data.
- *Evaluation of credentials of employees every time a new access is performed*

  YES: For key generation, PKG will be an authorized agent responsible for the generation of master key, device parameters, sharing of a secret key and public key to patients, research institutions and hospitals.
- *Citizen's level of control over their data access and privacy*

  MEDIUM: patient can own and share his personal data to all nodes of the implemented permissioned blockchain
- *Level of security of the authentication system used every time a new access is performed*

  HIGH: It will create a blockchain address (ADDR) according to users' roles and issue various permissions such as Enrolments Cert and Transaction Cert based on those participants' ID's.

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES: any node that joins to the network must reveal its role and identity
- *The distribution of access opportunities is not influenced by any form of contingencies*

  NO: to join to the network it is necessary to have a blockchain address which depends on users' role in the society
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  N/A: there is not any specification in the system implementation
- *Level of heterogeneity of the sources of the data used and analysed*

  HIGH: data comes from hospitals and the sharing of data by patients provide a financial compensation for them
- *Type of classification method used*

  ANTI-CLASSIFICATION: sensitive data are not used in any decision-making process

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

N/A: the system provides a storage directly in the blockchain but in an encrypted way

- *Use of approved cryptographic mechanisms to protect data stored*

  YES: the system provides a storage directly in the blockchain but in an encrypted way

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  MEDIUM: The interchange between the person named Pi and a research institution named Ri is documented by a transaction, and the information is provided and reviewed by PBFT-s protocol.

- *Type of responsibility implemented*

  TRIADIC: any exchange of information between parties is documented

- *Volume of responsibility defined*

  SOLE: any exchange of information between parties is documented

6) hOCBS

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: since data come from hospitals

- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  YES: is guaranteed through verifiable Off-chain Computations with cryptographic proofs, which ensure the integrity and correctness of them upon being written to the blockchain

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: verifying the owner approval of its own data sharing while maintaining anonymity

- *Evaluation of credentials of employees every time a new access is performed*

  YES

- *Citizen's level of control over their data access and privacy*

  HIGH: security is added by verifying the owner approval of its own data sharing while maintaining anonymity

- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: A digital wallet, a type of distributed application (Dapp) that holds verifiable credentials about an identity and enables the signing and submitting of a transaction through an off-chain construct (e.g. private keys), will authorize healthcare data-related transactions in a secure and patient-centric manner

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES
- *The distribution of access opportunities is not influenced by any form of contingencies*

  NO: This framework uses the Proof of Authority as a consensus mechanism and it becomes in contrast with the ethic requirement of Fairness, since this method gives rise to an identification of a limited number of participants which have the power to validate transactions and interactions all over the network
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  NO: sensitive data are not used to assess the necessity of some compensatory tools
- *Level of heterogeneity of the sources of the data used and analysed*

  HIGH: there is the distinction of three different parts of healthcare data which are protected, genomics and consumer health information
- *Type of classification method used*

  ANTI-CLASSIFICATION

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  YES: storage of data is performed off-chain
- *Use of approved cryptographic mechanisms to protect data stored*

  YES

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  MEDIUM: any time a new access is performed some identifiable credentials are asked to the user
- *Type of responsibility implemented*

MONADIC

- *Volume of responsibility defined*

  SOLE: any time a new access is performed some identifiable credentials are asked to the user

7) MedicalChain

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES

- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  YES

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: A dynamic system has been developed that identifies actors and gives them the appropriate scope over a health record, contingent on the patient's permission.

- *Evaluation of credentials of employees every time a new access is performed*

  YES: Civic identifies and verifies users using biometrics, which provides a simple and safe way of ensuring user's privacy.

- *Citizen's level of control over their data access and privacy*

  HIGH: patient can define who is authorized to access and modify data

- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: Civic identifies and verifies users using biometrics, which provides a simple

  and safe way of ensuring user's privacy.

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES: Right to Justification: no relationships or accounts should exist if they are not adequately justified towards those involved. Additionally, every actor has the right to demand justification for the treatment he is subjected to.

- *The distribution of access opportunities is not influenced by any form of contingencies*

NO: user capability to provide different levels of access and to design who can query and write data on the blockchain

- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  NO: there is not any system that allow an evaluation of the necessity to have some compensatory tools
- *Level of heterogeneity of the sources of the data used and analysed*

  HIGH: data come from HER
- *Type of classification method used*

  ANTI-CLASSIFICATION

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  NO: there is not any indication about the possibility to store data off chain,
- *Use of approved cryptographic mechanisms to protect data stored*

  YES

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  HIGH: transparency on data is rewarded through MedToken
- *Type of responsibility implemented*

  TRIADIC: due to the possibility to implement telemedicine
- *Volume of responsibility defined*

  SOLE

8) MedRec

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: The metadata contains information about ownership, permission and the integrity of the data being requested
- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  NO: there is not the implementation of an interacted

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: When a patient requests access to a particular medical record, it sends a request and the Database Gatekeeper implements an access interface to the patient node's local database, governed by permissions stored on the blockchain.
- *Evaluation of credentials of employees every time a new access is performed*

  YES: MedRec is this private client that defines a Global Registrar (a contract mapping all public identities to Ethereum addresses), ensuring that only registered healthcare providers are permitted to append blocks to the MedRec blockchain
- *Citizen's level of control over their data access and privacy*

  HIGH: patient can also select the portion of data which is possible to visualize by all the other nodes of the blockchain
- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: The Database Gatekeeper implements an access interface to the patient node's local database, governed by permissions stored on the blockchain. The Gatekeeper runs a server listening to query requests, which are cryptographically signed by the issuer, from clients on the network. The cryptographic signature allows the gatekeeper to confirm identities, and then check the blockchain contracts to verify if the address issuing the request is allowed access to the query.

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES: The patient provider relationship contract links two nodes in the system, where one node stores and manages medical records for the other. This relationship could exist between a particular care provider and patient but extends to cover any pairwise data stewardship interaction.
- *The distribution of access opportunities is not influenced by any form of contingencies*

  YES: once nodes are verified and identified, there is not any distinction between them
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  N/A: there is not any information about the application of some compensatory tools according to the type of sensitive data processed
- *Level of heterogeneity of the sources of the data used and analysed*

HIGH: data comes from HER

- *Type of classification method used*

  ANTI-CLASSIFICATION: protected categories, such as race and gender, are not explicitly used in decision making

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  YES

- *Use of approved cryptographic mechanisms to protect data stored*

  YES

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  HIGH: The summary contract serves as a trail of breadcrumbs, where each participant in the system can locate a summary of their relationships with each other participant. The summary contract encodes a list of references to Patient-Provider Relationship contracts, giving both current and previous engagements with other nodes on the system. Each relationship also stores a 'status' variable, indicating when the relationship was established, and whether it has been approved by the patient.

- *Type of responsibility implemented*

  TRIADIC: due to the presence of summary contracts

- *Volume of responsibility defined*

  SOLE: due to the presence of summary contracts

9) Akbar proposal

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: all data come from hospital and EHR

- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  YES: Accuracy of data is guaranteed by testing data integrity and the result given by this kind of examination is useful to determine whether the smart contract, that has been stored on the Ethereum network, will experience changes caused by parties during the deployment process.

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: there is the implementation of Web Services, which facilitate interaction between users and system that has been created.
- *Evaluation of credentials of employees every time a new access is performed*

  YES: since this system is based on the implementation of a private blockchain
- *Citizen's level of control over their data access and privacy*

  HIGH: data access is analysed though a data sharing test, which allows to determine whether an hospital can access to data owned by another one.
- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: the authentication system is implemented through smart contracts

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES: it is possible through the data sharing test, which allows to determine whether an hospital can access to data owned by another one.
- *The distribution of access opportunities is not influenced by any form of contingencies*

  NO: due to the implementation of a private blockchain, where only the first node has the right to mine
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  NO: there is not the possibility to assess the necessity to require some compensatory tools from nodes.
- *Level of heterogeneity of the sources of the data used and analysed*

  HIGH: The results of the scalability test are to ensure that the system can cope with the heavy loads that are directed at the system itself
- *Type of classification method used*

  ANTI-CLASSIFICATION

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  NO: data are stored on blockchain, but the security is ensured through the implementation of cryptographic techniques

- *Use of approved cryptographic mechanisms to protect data stored*
  YES

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*
  HIGH: since the system is based on the implementation of a private blockchain, the level of accountability of participants will be high
- *Type of responsibility implemented*
  MONADIC: it considers the general concept of responsibility
- *Volume of responsibility defined*
  SOLE: due to the implementation of a private blockchain

10) Sun proposal

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*
  YES: when a patient goes to the doctor, he gives to him the certificate in order to generate his personal medical data
- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*
  YES: a digital signature of the doctor and the patient is applied on medical record.

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*
  YES: the new scheme allows doctors and patients to set the policy about who has the right to access EMRs for realizing more secure data management and resisting data forgery
- *Evaluation of credentials of employees every time a new access is performed*
  YES: Data Access is performed by implementing an Attribute-Based Encryption (ABE), which enables doctors and patients to state if data requestors have attributes to decrypt EMR.
- *Citizen's level of control over their data access and privacy*
  HIGH: Every data is accompanied with a data sharing test, which allows to determine whether an hospital can access to data owned by another one.
- *Level of security of the authentication system used every time a new access is performed*

MEDIUM

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES
- *The distribution of access opportunities is not influenced by any form of contingencies*

  YES: once the requestor is authenticated, there is not any form of contingencies that influence the access opportunities
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

  NO
- *Level of heterogeneity of the sources of the data used and analysed*

  HIGH: data come from any type of medical records
- *Type of classification method used*

  ANTI-CLASSIFICATION

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*

  YES: data storage in the IPFS, where data can be modified and deleted whenever it is required
- *Use of approved cryptographic mechanisms to protect data stored*

  YES: The ciphertext generated is made of two parts, the first one deals with the EHR, and it is stored in the IPFS, while the second part includes the keyword used between the two mentioned entities and so, it is stored inside the smart contract

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*

  LOW: each transaction gives as output different public-private key pairs, which protects the identity of requesters
- *Type of responsibility implemented*

  MONADIC
- *Volume of responsibility defined*

  SPHERE: due to the anonymity of actors in a transaction

11) Trough proposal

➔ **Accuracy**

- *Every data is accompanied with a datasheet describing its operating characteristics*

  YES: Data activities should be logged in a distributed ledger. The logs should contain information about 'who', 'why', 'when', 'what' and 'how' personal data was processed
- *Every tool has an interacted visual surface which allows the data owner to evaluate the correctness of information before managing them*

  YES: the platform always requires DS's signature for data collection or for granting consent.

➔ **Data governance and privacy**

- *There is a system that avoid collecting or run a set of data if no consent has been given*

  YES: only authorized Service Provider receives an access token, which is a sort of proof of permission showing that a party is granted to access to a particular dataset
- *Evaluation of credentials of employees every time a new access is performed*

  YES: the Server Provider performs an access request to the blockchain platform, which plays a role of a delegated authentication and authorization server.
- *Citizen's level of control over their data access and privacy*

  HIGH: data owners have full permissions to manage data usage policy
- *Level of security of the authentication system used every time a new access is performed*

  MEDIUM: Security of the identity, authentication and authorisation mechanisms, which depends on the security of the cryptographic primitives, is assumed to be secure.

➔ **Fairness**

- *The system complies with the Right to Justification*

  YES
- *The distribution of access opportunities is not influenced by any form of contingencies*

  YES: once nodes are identified, the access opportunities are not influenced by any form of contingencies
- *Sensitive data are used to evaluate the necessity to require some compensatory tools*

NO

- *Level of heterogeneity of the sources of the data used and analysed*
  HIGH: data come from medical records
- *Type of classification method used*
  ANTI-CLASSIFICATION

➔ **Right to be forgotten**

- *The use of sensitive data takes place in standalone systems disconnected from the network*
  YES: data are stored off chain
- *Use of approved cryptographic mechanisms to protect data stored*
  YES

➔ **Responsibility**

- *Level of accountability of participants and of any form of outcome of the system*
  HIGH: The platform not only provides mechanisms for DS rights but also plays as a role of a DC for handling personal data processing and demonstrating data accountability. By honestly participating in the BC-based personal data management platform, an SP can be endorsed by the BC network that it is GDPR-compliant. Otherwise, any violations are recorded in an immutable distributed ledger as a record of the infringements, which can be then used for the GDPR compliance investigation by supervisory authorities.
- *Type of responsibility implemented*
  TRIADIC
- *Volume of responsibility defined*
  SOLE