EU Blockchain
Observatory and Forum

# Blockchain Applications in the Healthcare Sector

A Thematic Report Prepared By
The European Union Blockchain Observatory & Forum

An initiative of the European Commission

## About this report

This is the fifth thematic report prepared by the team leading the EU Blockchain Observatory and Forum, aiming to present the latest developments, use cases and applications of blockchain in the healthcare sector as well as in the COVID-19 pandemic management.

This is part of the series of reports that will be published addressing selected topics in accordance with the European Commission priorities.

## Credits

This report has been produced by the EU Blockchain Observatory and Forum team. Written by:

- **Kristina Livitckaia**, **Iordanis Papoutsoglou**, **Konstantinos Votis**, Centre for Research & Technology Hellas
- **Wendy Charles**, Life Sciences Division, BurstIQ, Inc. & Faculty, Business School, University of Colorado
- **Urko Larrañaga Piedra**, Izertis S.A
- **Matthew Niemerg**, Aleph Zero Foundation
- **Anton Hasselgren**, Faculty of Medicine and Health Science, Norwegian University of Science and Technology
- **Elsa Papadopoulou**, Department of Informatics, Ionian University

Several sections of this report are driven by the interviews with the following experts in the domain:

- **Nenad Georgiev**, Nordic Entertainment Group
- **Robert Chu**, Embleema
- **Marco Cuomo**, Novartis Pharmaceuticals

*In this report preparation, we would like to acknowledge the guidance and all-time support of **Tonia Damvakeraki, INTRASOFT International**. Special thanks to **Scope** for the editorial review and language proofing. We thank **Ismael Arribas, EU Blockchain Observatory and Forum Expert Panel** for brainstorming and conceptual discussions.*

## Note

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this paper.

## Disclaimer

# Contents

# CHAPTER 1. BLOCKCHAIN IN HEALTHCARE

## 1.1 CHALLENGES IN THE HEALTHCARE INDUSTRY

The healthcare industry faces challenges due to constantly changing conditions, including demographic transitions and the advancements we have achieved until now in health science and the healthcare industry. Life expectancy has increased, and we live longer with chronic diseases (Anderson & Hussey, 2000; Bongaart *et al*., 2015). This requires the healthcare industry to focus on an increasingly older population with a more complex disease burden than healthcare previously dealt with. As a direct consequence of the demographic shift, non-communicable and chronic diseases are becoming more prevalent, straining all health systems (Harris, 2019). New methods, procedures, and financing mechanisms are necessary to have a sustainable health system in the future (Morgan, Zamora & Hindmarsh, 2007).

As healthcare has developed and started to adapt new digital methods and tools, more effective remedies - both within primary prevention and in the field of curative, technology-intensive medicine have been introduced (Gopal *et al*., 2019). This transition is often referred to as digital transformation, which involves a shift from paper-based medical records to electronic records and new technologies to improve healthcare and patient engagement (Massaro, 2021). Yet, further application of new technology solutions and approaches, including the use of blockchain, is of high value to contribute to the prevailing demands in the industry and partially support further transformation and digitalisation of healthcare (Hasselgren *et al*., 2020). Below, we discuss some of the remaining challenges in the healthcare industry, and later in this chapter, address how blockchain could be used to facilitate the necessary changes.

Below we list some of the challenges the healthcare industry is facing. This is not an exhaustive list, but it includes the most evident challenges. While technology challenges could potentially be addressed with new digital technologies, including blockchain technology solutions, we start with points that might prevent the adoption of new technologies and approaches, including organisational and patient engagement perspectives.

### Organisational and workforce challenges

- The more advanced methods and tools have increased **demand for the education and training of health personnel** and increased specialisation. The amount of knowledge a healthcare professional needs to remain up to date increases exponentially (Illingworth & Chelvanayagam, 2017).

- The increased specialisation has enhanced the demand for effective triage and more effective tools for **multi-disciplinary collaboration**. These collaborations need to be expanded across disciplines and outside of the healthcare sector (Keys, Silverman & Evans, 2017).

- The vastly broadened repertoire of healthcare-related knowledge, methods, and tools that have been utilised have brought **more complexity to the healthcare system**. In fragile healthcare systems, this complexity renders systems more prone to errors (Braithwaite *et al*., 2017).

- The need for a more **effective distribution of knowledge and data** has enhanced the demand for tools that boost coordination and improve the function of healthcare systems. This has brought solutions such as health registries, electronic health record systems, clinical decision-support systems, workflow support systems, and other systems that build upon a knowledge infrastructure.

- Healthcare organisations tend to be **slow in adopting new technologies**. Adoption is influenced by assessments of feasibility, cost-effectiveness, profitability, and potential success (Tal, Booch & Bar-Yehuda, 2019). Technology evaluations involve a complex, multi-disciplinary approach that reflects organisational politics, as well as the organisation's values (Tal, Booch & Bar-Yehuda, 2019).

### Patient engagement with health information challenges

- Patient engagement involves **empowering patients** to take an active role in their disease and healthcare management to improve wellness (Tobiano, Jerofke-Owen & Marshall, 2021). Using tools and technologies to interact with health information is a critical component of patient engagement (Clavel *et al*., 2021).

- Not all patients have **sufficient access to technology**. More than ever before, a higher percentage of individuals own computer devices and have access to the internet[1], but there are still populations that lack access to broadband and affordable computing devices (Brall, Schröder-Bäck & Maeckelberghe, 2019).

- Some individuals do not have **sufficient language literacy or technology proficiencies** to interact with digital health information (Brall, Schröder-Bäck & Maeckelberghe, 2019).

- The transition to **virtual healthcare service** might present **trust challenges** when the physical attributes tied to the physical appearance of healthcare professionals and facilities disappear (Hasselgren *et al*., 2021).

- As a **patient engagement paradox**, patients report interest in accessing their health information through a patient portal or app. However, only around 30% of patients actually access their health information (Allard & Krasowski, 2021; Son *et al*., 2021). The likelihood and nature of access depend on the demographic factors of gender, marital status, education, and having a regular physician (El-Toukhy *et al*., 2020), as well as age and primary language (Allard & Krasowski, 2021). Additional technology factors are listed below.

### Technology challenges

- Health system **interoperability** is the ability for different health information technology systems (both between and within organisations) to integrate and exchange data for improved healthcare delivery (Zhang *et al*., 2018). Interoperability involves foundational, structural and semantic (vocabulary/terminology), and organisational requirements (Health Information and Management Systems Society, 2020). While there is increasing use of standards for interoperability, healthcare interoperability is still far from reality, and blockchain technologies are currently being used to assist organisations with their interoperability efforts (Zhang *et al*., 2018).

- Perceived **usability** and usefulness of health information systems: Both healthcare providers and patients are less likely to interact with health information systems if the systems do not offer ease of interaction and access to the system (Son *et al*., 2021).

[1] The Pew Charitable Trusts. (2021). How FDA Regulates Artificial Intelligence in Medical Products. Source.

- The **transparency** of the knowledge and data stored in these systems is often siloed (Nelson & Staggers, 2016), and organisations seek secure methods of aggregating and utilising data for healthcare research, operations, and quality control (Porsdam Mann *et al*., 2021).

- Computationally enhanced sensor and imaging capturing devices have enabled clearer depictions of each patient's disease as well as facilitated the development of minimally invasive techniques (e.g., minimally invasive surgery, ablation therapy). This creates challenges for **managing**, **interoperating**, and **utilising data** associated with these sensors (Comaniciu *et al*., 2016).

The challenges presented here are not comprehensive of all challenges facing healthcare systems and organisations. The challenges vary depending on the healthcare system from various perspectives, including health-improving activities, financing mechanisms, socio-economic circumstances, and other factors unique to a specific country or region (Gopal *et al*., 2019). But as the COVID-19 pandemic has shown us, the resilience of all healthcare systems across the globe remains fragile; we face common challenges when it comes to population growth, demographic shift, and infodemic consequences.

As the healthcare system is currently being digitally transformed, it can be considered more decentralised by its nature. For instance, health-related data are being collected by more and more devices controlled by individuals. Patients can seek health services from a larger selection of health service providers, including providers outside the normal jurisdiction of the patients, and medicines can be ordered from an increased number of digital pharmacies. While blockchain technologies do not aim to address every challenge related to health information, this decentralised shift fits well with decentralised technologies such as blockchain and distributed ledger technologies.

## 1.2 BLOCKCHAIN APPLICATIONS FOR HEALTHCARE DATA & TRANSPARENCY

Blockchain-based technologies have been increasingly explored as an approach to health information technology, and the process is ongoing. When introducing nearly any new technology, healthcare professionals' perceptions range from excitement to scepticism. When used for healthcare, **blockchains combine** data storage, encryption, and distribution in a new way to protect health information (Joshi & Gokhale, 2021) and require a flexible mindset that differs from the transparent blockchains used for value transfer. Blockchain technologies designed for health information may be best represented as a set of technology tools without a limiting definition (Zheng *et al*., 2017). Since technologies that process health information must maintain the privacy of that information, early blockchain technologies designed for healthcare are focused on private, permissioned blockchains, in contrast with the public, permissionless chains (Sharma, 2019). Some individuals entrenched in public blockchain designs questioned whether private ledger technologies could be considered "blockchains" (e.g., Lopez, Montresor & Datta, 2019). However, this binary differentiation is now largely antiquated (Charles, 2021b). For example, some public blockchains have evolved to include permissioned modules and governance layers, such as Private Ethereum and Enterprise Ethereum.

There are also concerns within the healthcare industry about blockchain "immutability." While blockchain technologies offer robust security, the National Institute of Standards and Technology (NIST) instead encourages the use of the term "**tamper-resistant and tamper-evident**" (Yaga *et al*., 2018). Specifically,

> *"Most publications on blockchain technology describe blockchain ledgers as being immutable. However, this is not strictly true. They are tamper evident and tamper resistant, which is a reason they are trusted for financial transactions. They cannot be considered completely*

> *immutable because there are situations in which the blockchain can be modified*" (Yaga *et al*., 2018, p. 34)

It is imperative for healthcare and life science organisations to consider the **software development life cycle** (Lilani *et al*., 2020) and the potential need to **archive data for long-term retention** (Bhatia & Wright de Hernandez, 2019).

Ultimately, there are roles for all permissioned and permissionless blockchain technologies in healthcare, and distinctions between current platforms will become increasingly nuanced (Charles, 2021a). It is also valuable to consider the wide range of verticals within the healthcare industry and that there are unique benefits and constraints to each application of blockchain technology (Allen *et al*., 2020).

As humanity moves further into the 21st century, the **digitalisation of all data** increases, including medical data (Tresp *et al*., 2016). Healthcare professionals and industry specialists are forced to increasingly **improve internal security policies** to ensure the security of Electronic Health Records (EHRs) or Electronic Medical Records (EMRs). The primary challenges of digitising EHRs or EMRs can be divided into two categories: **data security** and **data interoperability** (Al-Issa *et al*., 2019). While of practical importance due to the growing number of private sector actors providing distinct EMR or EHR solutions, interoperability of data between these systems is not a cybersecurity concern. Instead, it is a **data standards problem** to ensure compatibility of patient records between any solution. Further, this section outlines how various primitives of blockchain technologies (and related technologies) can be used by EHR or EMR systems to mitigate the problems of the former category.

A properly designed healthcare application on a **distributed ledger** can **alleviate** many of the **concerns** surrounding **data security**, concerning three aspects: **storing data** securely, the **authorised reading**, and **writing** of the data. Distributed data storage can be deployed in such a way that no single data centre has a direct copy of the underlying patient data. This is either in an encrypted format or in raw text, using a common mathematical technique known as erasure codes first introduced in the middle of the 20th century (Hamming, 1950). Storing and reading data using erasure codes has been widely used by many technologies since the late 1970s. This includes CD-ROMs, DVDs, RAID, satellite communications, QR codes, fault tolerance in large data centres (Lin & Tzeng, 2010). Erasure codes work by dividing the data into *n* equally sized pieces and adding extra **redundancy information** to each chopped-up piece. Then, depending on the particular erasure code, a specified *k* of these *n* pieces of data can be used to reconstruct the original data. Erasure codes are a powerful technique that allows data controllers and processors to achieve a high degree of data security (L'Hutereau *et al*., 2019). In the most extreme and secure setting, *n* different data chunks would be stored at *n* different data centres. Therefore, to obtain control of the original data, an attacker must gain access to *k* of the data centres (and, potentially, *k* different private keys used for encrypting the underlying data) instead of only one.

Storing large amounts of **patient data on a blockchain** can be challenging to manage, regardless of whether the distributed ledger operates as a permissioned or public network (Opportunities and Challenges of Blockchain Technologies in Healthcare, 2020). Recording data on a blockchain using obfuscation techniques, such as **encrypting** or **hashing the data**, are industry-standard practises that reduce access to sensitive information (Zyskind, Nathan & Pentland, 2015). **Erasure codes**, another obfuscation method, could be employed by treating the blockchain as a modified distributed hash table that **stores the off-chain location of each of the data chunks** needed to reconstruct the original data. Second, maintaining **strict access control requirements** to authorised healthcare providers is complicated in emergency situations where the patient or a family member cannot consent to access records. In the practice of medical personnel, when such

occurrences happen, the supervising physician uses a personalised code to request access to the private records. Depending on the regulations within a particular jurisdiction, these records are stored for a limited time, and all access requests are logged accordingly.

### 1.2.1 Permissioned vs Permissionless

Blockchain networks can vary on the **permission** and participation openness of the network. Most applications set a process for accessing the network as permissions are in place to add another layer of protection due to the data sensitivity. Apart from the permission, networks are constructed around a private blockchain that defines validators following a policy. The consortium blockchain is referred to in the work of Eisenstadt *et al*. (2020) as a private blockchain created by the collaborations of various stakeholders. One of the prime candidates for technologies to support private chains with their packages and functionalities is Hyperledger, used in such solutions as DeepHealth (Rakib *et al*., 2021) or SPIN (Alabdulkarim *et al*., 2021). On the other hand, public blockchain finds uses in applications that support smart contracts (Rakib *et al*., 2021; Odoom *et al*., 2019). The key blockchain technology for such applications is Ethereum, as the Solidity programming language used for smart contract development is most notably used with Ethereum.

Despite using a public blockchain, personal and medical data is not aimed to be stored directly on the blockchain. The work of Nehme *et al*. (2021) comments on the approach of the blockchain acting as a Trust Anchor. The immutable ledger stores transactions with a timestamp and facilitates the recording of critical events on the network of cooperating parties. Personal and medical data are not exposed on the blockchain but rather kept off-chain. The solutions proposed by Odoom *et al.* (2019) and Abid *et al.* (2021) are to use the InterPlanetary File System (IPFS) for off-store data storage. Encryption methods producing a hash of the data provide the necessary information to store on the blockchain without storing the actual data.

Blockchain can support the high availability of applications due to its decentralised nature. If a node is active in the network, operations in the network are continuous without interruptions. The availability of services is vital for a particular application, such as certification (see 2.1.1 COVID-19 Vaccination Certificate Status) that needs to be constantly running. The service availability can be enhanced using distributed storage systems like IPFS used by Odoom *et al.* (2019) and Abid *et al*. (2021).

As previous research has shown, it is far more common for a permissioned private or consortium blockchain to be utilised in the healthcare space (Hasselgren *et al.*, 2020; Zheng *et al*., 2017). Although these works were published pre-pandemic and did not include use-cases such as vaccination certifications and contact-tracing apps, a public blockchain still might add value along with a private or consortium. The properties and distinction between public, private, and consortium can be summarised in a simplified table as follows (Zheng *et al*., 2017).

**Table 1.** Properties and distinction between public, private, and consortium blockchains

| Property / Type of blockchain | **Public blockchain** | **Consortium blockchain** | **Private blockchain** |
|---|---|---|---|
| **Consensus determination** | All validators | Selected set of nodes | One organisation |

| Property / Type of blockchain | Public blockchain | Consortium blockchain | Private blockchain |
|---|---|---|---|
| **Read permission** | Public | Public or restricted | Public or restricted |
| **Immutability** | Nearly impossible | Could be tampered | Could be tampered |
| **Efficiency** | Low | High | High |
| **Centralised** | No | Partial | Yes |
| **Consensus process** | Permissionless | Permissioned | Permissioned |

### 1.2.2 Public Key Infrastructure

A basic technology coupled with all blockchain systems is a decentralised **public key infrastructure** (**PKI**). It enables a central certificate provider to associate a digital identity or identities with a unique natural person (Maurer, 1996). PKI also provides strong **authentication** using cryptographic methods and has been widely used by enterprises for decades (Herzberg *et al*., 2000). PKI is the basis for some role-based access control models (RBAC) for file systems, encrypting files, secure electronic data transfers, authorisation, and verified credentials (see 2.2 USE OF VERIFIABLE CREDENTIALS IN COVID-19 PANDEMIC). Within blockchains, PKI is used to prove ownership of an account or address and is used at its simplest form for creating digital signatures for transactions that can be verified with the associated public key or address. Embedded within the logic of any smart contract are the rules of which identities, delineated by a list of public keys if the function is non-public, have the authority to interact with the smart contract. Granting access or emergency authorised use to any EMR or EHR data is solvable using PKI (Watts, Yu, & Yuan, 2010). Messages signed with an individual's private keys act as authorization proof to enable providers to read or update records. One advantage of PKI is granting private keys that are valid to access records for a limited time (Abadi *et al*., 1993). As such, individuals could grant temporary access (to read or update) to a specialist who is not the patient's regular primary healthcare provider.

Using PKI also allows authorised personnel emergency access to EHR or EMR data by maintaining a separate authorisation access list. PKI can even restrict emergency access or require a threshold of managers or supervisors to allow for such access. A hierarchical PKI would allow flexibility to add or remove the appropriate personnel to these lists within a particular hospital system or network. By requiring that all EMRs or EHRs **store an access log**, a blockchain system can help to ensure no unauthorised access occurs and **flag suspicious access in real-time** using machine learning (ML) and alert members within an organisation (Stolfo *et al*., 2005). Blockchain with PKI also allows an EMR or EHR to maintain a list of cryptographic proofs for every update to the underlying record by requiring the authorised healthcare provider to sign the update

digitally. Importantly, **access and update logs** can be publicly maintained **without disclosing** a patient's name, the provider's name, or the actual content of the EHR or EMR using obfuscation techniques, thus providing a greater degree of accountability and transparency to how private healthcare data is managed (Zyskind, Nathan & Pentland, 2015).

Over the last several decades, different mathematical techniques have been developed that exist independent of blockchains that might be valuable in solving the data challenges surrounding medical or healthcare data. These mathematical tools, namely **erasure codes** and **cryptographic signatures** have been applied in a wide range of commercial settings (Plank & Thomason, 2003; Katz, 2010), and the underlying principles are well-understood. As blockchain technology development continues, these standalone mathematical tools form an integral component within distributed ledger technologies, and their combined use is often not found in other technology stacks.

**Privacy** is a fundamental concept in the applications in the literature. **SPIN** (Alabdulkarim *et al*., 2021) is a blockchain-based framework that includes a cross-border application to share information between countries. SPIN adopts a PKI method based on blockchain for communication, preserving privacy by checking access rights. The underlying network relies on the definition of a peer in each country to enrol and authenticate users. **DeepHealth** (Rakib *et al*., 2021) uses the blockchain's ledger to preserve and provide privacy. Any action on the users' data can be regarded as a transaction stored in the ledger. Audits on the entities and procedures accessed the data are possible and accurate as the ledger is immutable to any malicious change. Pseudo-anonymisation is a method to preserve the participants' privacy while sharing information in a network. For example, the work of Yu *et al*. (2020) implements such a method for the privacy of identities. Pseudo-anonymisation can protect from **cyber-threats** like inference attacks that deduct information from the exchanged packages.

## 1.3 BLOCKCHAIN APPLICATIONS FOR PHARMACEUTICAL AND HEALTHCARE SUPPLY CHAIN

The impact of the blockchain on the supply chain in the pharmaceutical industry and healthcare is shown to be one of the most evident use cases, where **traceability** and **transparency** are key data elements.[2] There are numerous parties involved in each phase of the supply chain process rendering a complex ecosystem. Yet, information sharing is asymmetrical, and updates usually reach network shareholders with a time lag. Furthermore, it is common to duplicate tasks and information due to the **silos**. Blockchain can disrupt the healthcare supply chain, noted by Singhal and Carlton from McKinsey & Company (2019), as it can increase the efficiency of the procedures.[3]

The European Commission (EC) (2020) has published a pharmaceutical strategy for Europe, supporting the perspective of the strategic actions to be taken.[4] While the strategy does not explicitly discuss blockchain as a solution, blockchain technology could assist several actions and concerns, including silos and transparency, as noted in the report. Another work from McKinsey & Company by Ebel, Larsen, and Shah (2013) is a five-

[2] Deloitte. (2017). Using blockchain to drive supply chain transparency. Source.
[3] McKinsey. (2019). The era of exponential improvement in healthcare? Source.
[4] European Commission. (2020). Pharmaceutical Strategy for Europe. Source.

step plan to strengthen the healthcare supply chain, sharing a similar perspective on the concerns discussed by the EC.[5]

In 2017, PricewaterhouseCoopers (PwC) documented general advantages of blockchain, including complexity, costs, and errors reduction, data security and resilience, and transparency.[6] As the deployment of applications has resulted in accumulating more experience, the use cases in the pharmaceutical industry have become more self-evident. Blockchain could facilitate the alignment and data transparency between all the stakeholders concerning **finished goods traceability** but also be utilised as **anti-counterfeiting** technology. For example, the World Health Organization (WHO) estimates that 10% of medical products are falsified[7], highlighting the demand for such use cases and even considering that blockchains could support the operation of processes more safely and efficiently[8]. However, regardless of the supply chain being a chain of custody process overall, some use cases might have very specific settings. For example, a **biological sample supply chain**, such as the **blood supply chain**, must be managed with its unique demands (Williamson & Devine, 2013). An efficient supply chain for demanding invaluable items like blood is vital, and blockchain can alleviate inefficiencies. There is an increasing number of solutions proposed, including the one introduced by Sadri, Shahzad, & Zhang (2021), such as an end-to-end system for tracking blood supply.

Recently, while the pandemic was overflowing, IBM researched four use cases for the pharmaceutical industry on the blockchain for **cold chain monitoring**, **provenance authentication** against fraud and theft, **reduced time and cost** due to digitalisation, and support regulations for **drug tracking**[9]. The latter use case is indeed brought up by many experts and researchers in the field, proposing more complex solutions that could support drug traceability, for example, using IoT devices (Nawale & Konapure, 2021). Overall, IoT devices can enhance control in the supply chain process allowing quality management throughout the chain.[10] Blockchain can act as a layer between the different entities and devices that facilitate communication and trust in the network (Kumar & Sharma, 2021). Moreover, most applications suggest deploying a **permissioned** blockchain network while maintaining a hash of the drugs on the blockchain for traceability reasons (Nawale & Konapure, 2021; Uddin *et al*., 2021). The hash is on the distributed ledger rendering real-time audits in any phase of the supply chain.

When analysing how blockchain technology could be adopted within the pharmaceutical industry in general, **system architecture**, clarity on the **transactions**, **governance** in the network, and, as a result, solution **deployment** are vital aspects in adoption to stakeholders involved in the process, so the solution brings its value to all participants involved[11]. This calls attention to the need for the development cycle to start with **requirements** definition at the initial development phase to guide all following actions. To structure the development, 10 non-technical requirements are noted in the work of Khatter (2021). Based on this work, consideration should be given to **interoperability** and **latency** due to common practice to integrate other technologies, like the Internet of Things (IoT), in supply chain applications. Other requirements introduce traceability, scalability, integrity, confidentiality, availability, security, performance, throughput, and trust.

[5] McKinsey. (2013). Strengthening health care's supply chain: A five-step plan. Source.
[6] PwC. (2017). How blockchain could strengthen the pharmaceutical supply chain. Source.
[7] WHO. (2017, 28 November). 1 in 10 medical products in developing countries is substandard or falsified. Source.
[8] Harvard Business Review. (2020). Why Big Pharma Is Betting on Blockchain. Source.
[9] IBM. The pharmaceutical industry on blockchain. Source.
[10] BLUMEglobal. How the Internet of Things Is Transforming Supply Chain Management. Source.
[11] PwC. (2017). How blockchain could strengthen the pharmaceutical supply chain. Source.

## 1.4 BLOCKCHAIN IN MEDICAL CREDENTIALING

The credentialing of healthcare professionals adds to the administrative burden of both clinicians and healthcare providers. As such credentials often are siloed at different institutes and agencies, the verifications of such credentials usually take time and resources, especially when healthcare professionals tend to shift with other employees and regions of work more often than before. Several initiatives have tried to address this issue with blockchain solutions, such as **ProCredEx** by Hashed Health (Hashed Health, 2020) and Axuall, Inc & MetroHealth (PRnewswire, 2020). Hashed Health has developed a blockchain-based solution that enables faster onboarding and credentials verification. The latter plan includes enabling digital portfolios with documentation of a practitioner's education, speciality training and board certifications, licenses, sanctions or medical malpractice judgments, evaluations, work history, and hospital affiliation.

Such credential services have also been proposed in the academic literature (Kamel *et al*., 2018; Hasselgren *et al*., 2021) as a means for healthcare professionals to create a decentralised work-history portfolio that contains verifications of experiences, skills, and formal credentials. This portfolio could potentially be utilised in a virtual healthcare environment to establish trust with the patients and would be equivalent to paper-based documentation (such as diplomas and certificates) as its digital and decentralised work-history portfolio (Anderson *et al.*, 2009; Hasselgren *et al*., 2020). Moreover, such digitalised portfolios could also be utilised to minimise malpractice by making it unfeasible to vanish one's previous work history. It could also serve as a means for guiding patients to the healthcare professional with the right competence to deal with specific health issues. This is especially relevant for low prevalent diseases and health conditions where experts are few. However, with the virtualisation and telemedicine transformation, these highly specialised healthcare professionals can serve patients across the globe if the competence is paired with the need. Blockchain and other distributed technologies serve high value for such use cases.

## 1.5 OPPORTUNITIES AND CHALLENGES: EXPERT OPINIONS

For the purpose of this health report, we designed a survey to assess the vision of managers and experts working in the healthcare and pharmaceutical industry. The survey asked about opportunities and challenges of the blockchain in the healthcare and pharma industry and assessed blockchain applicability in COVID-19 response management.

The survey included 20 questions and targeted answers based on experts' professional roles and experience. The survey was held anonymously and on voluntary initiatives. The respondents were free to share their details (name and email address) if they were willing to be interviewed regarding the survey subject or be part of future surveys or initiatives related to blockchain in healthcare and pharma.

The survey results are based on 34 completed surveys. Most respondents work with the blockchain (79.4%) in pharma, research and academia, small and medium enterprises (SMEs) and start-ups, and healthcare service providers. Most of the respondents' organisations own the department or hold staff responsible for blockchain technologies (64.7%) and have already developed (55.9%) or deployed (52.9%) at least one blockchain solution.

Considering the opportunity of blockchain technology, the respondents rated the following applications as the most suitable for **technology utilisation serving high value** in the healthcare and pharma industry:

- Data transparency (91.1%)
- Medical and pharmaceutical supply chains (88.2%)

- Data immutability (85.3%)
- Collaboration between manufacturers, suppliers, retailers, and end consumers (85.3%)
- Medical records sharing (79.4%)
- Secure payment transactions (76.5%)
- Record accuracy (73.5%)
- Data interoperability (70.6%)
- Identity management (70.6%)
- The use of smart contracts for insurance purposes (67.7%)
- Data management (61.7%).

While data transparency, immutability, and interoperability are the widely discussed needs across many domains when it comes to the use of blockchain (Capece & Passiatore; 2021; Ahram *et al*., 2017), supply chain and collaboration between the stakeholders are the use cases that especially got the attention during the pandemic (Khurshid, 2020; Kumar, 2020). Further, the respondents outlined several use cases that are related to the supply chain of goods, including anti-counterfeiting, product and material provenance, track and trace in personalised medicine, traceability of COVID-19 tests and vaccines and interconnection between several organisations for verification tests/vaccines, and clinical supply chain as part of the clinical trials. Focusing on the most promising use cases to **support pandemic management** and mitigate COVID-19 challenges, the respondents selected the following use cases:

- Transparency in pandemic data (67.7%)
- Supply of inventories of lifesaving drugs (67.7%)
- Quality of pandemic data (61.8%)
- Identity management (61.8%)
- Keeping track of COVID-19 data for vaccination (58.8%)
- Patient consent (55.9%)
- Clinical supply chain (52.9%).

Overall, based on the survey results, most of the respondents (79.4%) agreed that the COVID-19 pandemic management accelerated the process of exploring and adopting blockchain. Following up with the most promising solutions that the respondents are aware of that utilise the blockchain to support COVID-19 response actions include vaccination/immunity passport (85.3%), tracking vaccine delivery (85.3%), and identity verification (70.6%) (see Figure 1). On the other hand, the use of blockchain to support the digitalisation of telemedical laboratories (11.8%), monitoring of isolation (14.7%), and social distancing (5.9%) are not notable yet might serve value (Garg *et al*., 2020). Further in this report, we dedicate a chapter focusing on the blockchain in pandemic management (see CHAPTER 2. THE ROLE OF BLOCKCHAIN IN COVID-19 PANDEMIC MANAGEMENT).

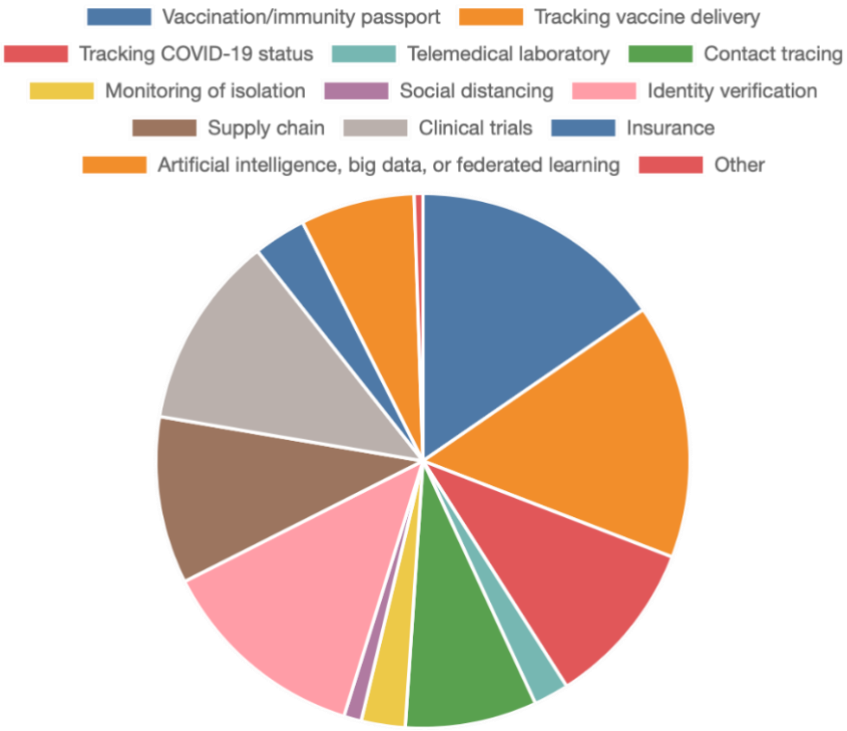


**Figure 1: Solutions to use blockchain in COVID-19 response actions**

As discussed throughout this report, the blockchain serves many possibilities for the industry from different angles and applicability perspectives. Still, as more complex use cases are approached, more complex and complete solutions are required, which might involve a blend of technologies (Abbas & Sung-Bong, 2019). For example, the results of the survey showed that the majority of experts believe that Artificial Intelligence (AI) (76.5%), Internet of Things (IoT) (76.5%), and Cloud Computing (52.9%) might serve **successful synergies for data utilisation** (see Figure 2).

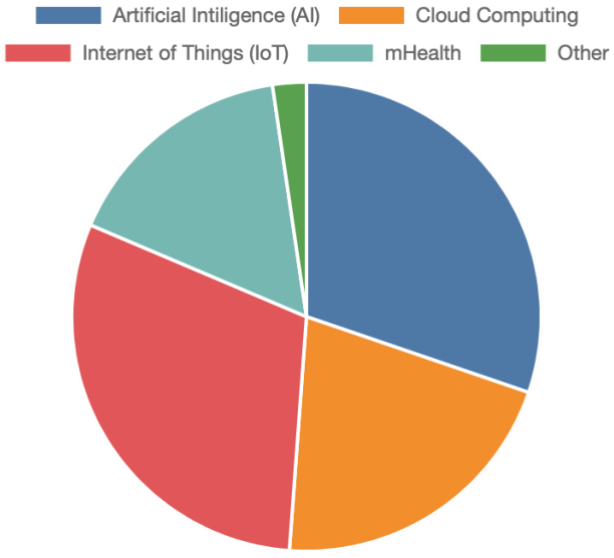


**Figure 2: Synergies with other technologies for data utilisation**

Based on the experts' responses, to support the utilisation of the solutions would require regulations and policies supporting innovation (82.4%), more and more reliable studies analysing the outcome of technology application (67.7%), skills training for solutions development (61.8%), and staff and patient education (55.9%) (see Figure 3).

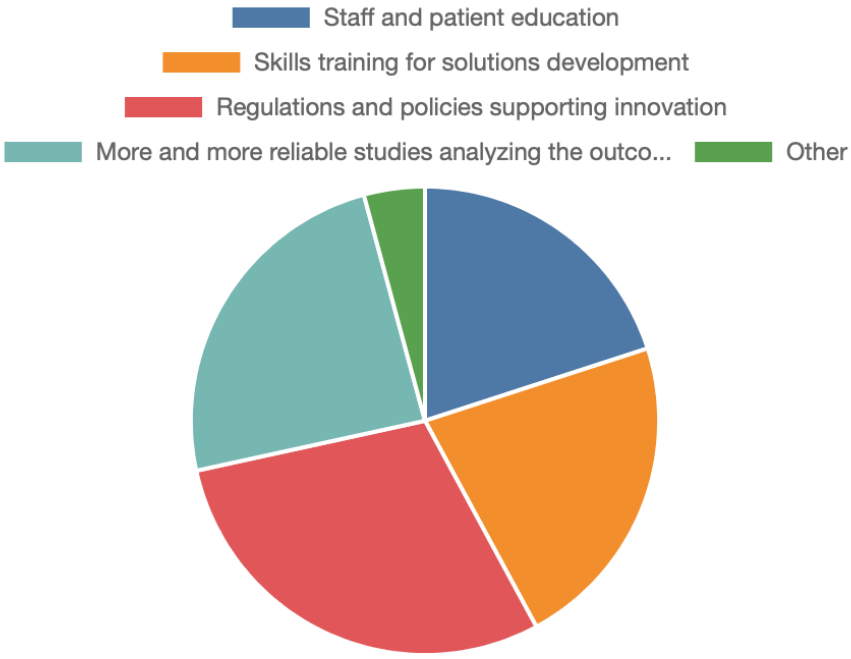


**Figure 3: Measures to support the utilisation of blockchain solutions**

And while the blockchain can be utilised for a large number of use cases along with the synergies with other technologies, some aspects might prevent the adoption of blockchain-based solutions in the healthcare and pharma industry, which we already preliminary discussed earlier in this chapter (see 1.1 CHALLENGES IN THE HEALTHCARE INDUSTRY). To extend the scope, below we include the **potential barriers** based on the survey results, including:

- Scalability issues (61.8%)
- Adoption by end-users (58.8%)
- Lack of government support (58.8%)
- Need for policy considerations for deploying blockchain (58.8%)
- Lack of awareness on such solutions (58.8%)
- Maintenance (55.9%)
- Technical challenges (52.9%)
- Cost of operations (52.9%).

At the same time, we found several rather controversial factors based on the responses. For example, privacy concerns (35.3% vs 44.1%), sustainability concerns (47% vs 32.4%), and performance (47% vs 38.2%) are considered as aspects not preventing the adoption, but at the same time, those might prevent. However, despite the barriers, most experts (82.3%) believe in the massive adoption of blockchain technology in the healthcare or pharma industry in the following five to 10 years.

# CHAPTER 2. THE ROLE OF BLOCKCHAIN IN COVID-19 PANDEMIC MANAGEMENT

While blockchain adoption in healthcare in Europe and globally was initially limited by the technological and organisational barriers described in Chapter 1, the COVID-19 pandemic has accelerated interest and implementations of the technology. As the pandemic continues, various blockchain initiatives are being explored to manage better disease prevention and control (Kritikos, 2020). Although some blockchain-based innovations were created to extend the functioning based on the existing demands (such as supply chain monitoring), several blockchain-based solutions were designed to address the unique needs created by the pandemic (Ng *et al*., 2021). Specifically, blockchain-based solutions have been proposed or implemented to address movement monitoring, contact tracing, vaccination passports, public health surveillance, pandemic-related supply chains, and other relevant use cases (e.g., Kritikos, 2020; Marbouh *et al*., 2020; Nguyen *et al*., 2021; Ng *et al*., 2021; Vervoort, Guetter & Peters, 2021). While many blockchain technologies have not yet achieved widespread adoption in healthcare, several companies have advanced beyond pilot projects into full-scale production. It is also valuable to note that many blockchain solutions designed for healthcare have exceeded the basic blockchain components of distributed ledgers in offering sophisticated new features.

This chapter focuses on how blockchain could support pandemic management and discusses a sample of blockchain-based applications in different development stages.

## 2.1 BLOCKCHAIN APPLICATIONS FOR COVID-19 PANDEMIC MANAGEMENT

The pandemic was an event that aggravated underlying issues in the healthcare sector. The stock of medical products is limited, and countries rely on cross-border transactions to supply their stock. The disruption in the market was significant due to the pandemic, as the demand was unprecedented. Cross-border transactions need time to conclude, which was not the case during the pandemic. Furthermore, the demand pushed in picking vendors in a hurry without running the appropriate control to guarantee the quality of the products. Revocations of medical products resulted from the haste decisions during the pandemic.[12] News still includes revocation occurrences as covered by *The New York Times*, which notes that internet orders are susceptible to counterfeit products.[13]

Blockchain is a candidate technology for **alleviating healthcare issues** and some of the incidents during the pandemic. For example, blockchain can help fight counterfeit masks by providing a tracking and authentication system.[14] Moreover, blockchain can aid in deploying solutions for lifting the prohibitions and opening the economy. Such applications can be the vaccine supply chain[15] and health passports.[16] The following section aims to familiarise readers with the applications suggested in the literature along with crucial points in understanding blockchain. The subjects presented in the following section are the vaccination certificate status, contact tracing, and federated learning where blockchain could help against the COVID-19 pandemic.

[12] Harvard Business Review. (2020). Why Big Pharma Is Betting on Blockchain. Source.
[13] The Times New York. Counterfeit Covid Masks Are Still Sold Everywhere, Despite Misleading Claims. Source.
[14] Cointelegraph. (2020, 09 April). Blockchain to Authenticate Coronavirus-Response KN95 Face Masks From China. Source.
[15] World Economic Forum. (2020, 20 November). Using blockchain to monitor the COVID-19 vaccine supply chain. Source.
[16] World Economic Forum. (2020, 30 July). Could this COVID-19 'health passport' be the future of travel and events? Source.

### 2.1.1 COVID-19 Vaccination Certificate Status

To reduce the spread of COVID-19, countries-imposed lockdowns, resulting in stay-at-home orders and business closures and permitting only necessary activities. As lockdown is an extreme measure to slow down the pandemic, ways to ease the measures have been explored by numerous government bodies, organisations, and associations throughout the globe. One of the solutions found to be efficient is to issue certification by legal authorities—certificates during COVID-19 cover mainly the fact of vaccination and vaccination details, results of diagnostic tests, and as proof of naturally acquired immunity (Haque *et al*., 2021).

The academic literature argues for the digitalisation of certificates as the paper-based version has vulnerabilities that can compromise the certificates' objective. Blockchain appears to enable security and privacy while digitising the certificates (Abid *et al*., 2021). The differences between methods for issuing certificates are privacy-preserving, unforgeable, easy to administer, easily verifiable, scalable, and cost-effective (Eisenstadt *et al*., 2020). Such benefits promote the interest of public organisations and governments. However, one of the most critical aspects is compliance with existing regulations and many requirements when scaled to the European or a global level. Accordingly, the European Commission, together with the Member States, has implemented the **EU Digital COVID Certificate** system and extended it to third countries.[17] The system does not rely on blockchain technologies.

Generally, blockchain technology can support creating a network for issuing a certification with allocated roles in the network and verification options for using COVID-19 vaccination certificates and trusting its authenticity. A blockchain network is commonly composed of clients that report their transactions to the ledger and validators that secure the network operations and add blocks. Clients can have different identities depending on the transactions they desire to store on the blockchain. The literature (Eisenstadt *et al*., 2020; Rakib *et al*., 2021; Odoom *et al*., 2019) mainly accounts for three entities to operate in the network: the citizens as end-users, healthcare institutions as issuers of certifications, and authorities as verifiers. The **Novidchain** application (Abid *et al*., 2021) extends the roles to include the government as an authority in granting access to the network. More examples are addressed in 2.2 USE OF VERIFIABLE CREDENTIALS IN COVID-19 PANDEMIC.

To track vaccination status, some countries or large-scale organisations are utilising blockchain as the underlying technology to track vaccination status. The following are examples of blockchain-based digital health passports designed or utilised in the EU Member States.

**SICPA**[18], a Swiss company, and **Guardtime**[19] based in Estonia and Switzerland combined their technologies to provide blockchain-based tamper-proof certificates for health and vaccine status (SICPA, 2021).

In Spain, **Vottun**[20] rolled out a blockchain-based digital health passport in April 2020 for decentralised deployments. The Vottun Health Passport stores health attributes and credentials while preserving privacy and security. This health passport identity solution was identified by Gartner as an early leader in 2020 for COVID-19 solutions (Columbus, 2020).

[17] European Commission. EU Digital COVID Certificate. Source.
[18] SICPA. Source.
[19] Guardtime. Source.
[20] VOTTUN Health. Source.

**Amadeus**[21], a Madrid-based company, is an international reservation system used by 474 airlines. This ticketing system adopted IBM's Digital Health Pass. The blockchain authenticates vaccination credentials against each country's requirements for travel restrictions (Quito, 2021). The smartphone-based app does not store personal information on the blockchain and allows users to manage the information they wish to share. When the smartphone shows a QR code, the border or airport agents only see a notice of whether the traveller was cleared for travel. As of July 2021, six airlines had activated the Digital Health Pass, including Air Europa, French Bee, and Air Corsica, but other airlines were expected to activate the pass throughout 2021 (Quito, 2021).

### 2.1.2 Contact Tracing

Communicable diseases have emerged as one of the world's challenges based on the reports recently published by OECD[22] and Deloitte[23]. The recent pandemic caused by COVID-19 has been a powerful example of a virus' rapid spread throughout the globe. Efforts to combat the spread of the virus (without the vaccine available) immediately after it was identified as a world health emergency that posed serious challenges in maintaining life and processes as before. For this reason, social distancing and contact tracing of the positive cases were recognised and adopted as one of the measures to offset the virus' spread.

During this period, interest in blockchain technology grew. Considered promising and of high value, the technology was studied by many researchers who published their suggestions on deploying a contact tracing application based on blockchain. This section aims to present academic work in the literature and let the reader grasp the reasons, benefits, and considerations for contact tracing applications based on blockchain.

Before diving deeper into the contact tracing applications, it is important to note several general considerations for the deployment of such an application. First, the **sensitive data** used by the application are the first consideration (Osmanlliu *et al*., 2021). The second is security, as messages must be communicated within a **network of users** (Fitzsimons *et al*., 2020). The deployment of a tracing application necessitates the availability of geospatial data for the accurate definition of a person's location at any given time. Such data are sensitive and personal since a person's behavioural patterns can be delineated. For this reason, users can be hesitant to interact with such applications, as the security and privacy of data are vital for the end-users. The close contact definition calls for the application of a procedure that interrelates the geospatial data of multiple users to flag the ones that came into close contact with a positive case. Therefore, establishing secure and anonymised communication channels is crucial for a successful tracing application. For alleviating these considerations, blockchain is suggested as a solution to either store and grant access to data securely or establish a secure network.

Further, there are considerations in the blockchain adoption for a contact tracing application specifically (Lv *et al*., 2020). First to be considered are a data model and a pipeline. The data model sets the common ground on the data to make the data interoperable throughout the network. The data pipeline should map the procedures for storing data on- and off-chain. **Off-chain** storage is vital to secure the anonymisation and safety of sensitive data, similarly to private data in Identity Hub.[24] Another aspect to consider is the scalability in the computations as the procedures can be pushed towards the edge devices (such as IoT devices, including

[21] Amadeus Ticketing Platform. Source.
[22] OECD Library. (2020). Health at a Glance: Europe. Source.
[23] Deloitte. (2021). 2021 global health care outlook. Source.
[24] EBSI Documentation. (2021). Off-chain Storage. Source.

smartphones). The devices' computational capabilities can be limited, but the adoption of **fog computing** and **edge architectures** can ameliorate this limitation (Alsahli *et al*., 2021). Finally, public blockchain can be problematic as gas fees can be costly and preventive for public usage. The off-chain data storage can diminish the transactions with the blockchain since only the absolute critical events should be stored on the blockchain.

Different ideas on data sources are suggested for deploying a contact tracing application. Initially, smartphones can act as devices that store geospatial data and partially share them with the blockchain (Peng *et al*., 2021). An example is a **NausiChain** framework (Marotta *et al*., 2021) that validates the users' location with the interaction of smartphones and Wi-Fi access points. However, considerations on the trustworthiness of data can emerge during the pandemic, as users may try to tamper and consequently conceal their data. The work of Wen *et al*. (2021) considers the data trustworthiness suggests the data inclusion from third parties of transactional history or surveillance systems as sources to validate the user's data. Another source is social media applications that hold geospatial data for users, and contacting users is possible on such a platform. For example, Peng *et al*. (2021) apply a contact tracing application based on the WeChat application.

Researchers are using blockchain for a wide range of applications. The most appealing characteristic of the technology is the near-immutable storage of data that prevents the data from being tampered with or deleted. NausiChain (Marotta *et al*., 2021) switch the central database storage with blockchain, while (Wen *et al*., 2021) and (Peng *et al*., 2021) are storing the spatiotemporal data. The data storage on the blockchain is decentralised and permits network peers to have continuous access to the data. Additionally, a central authority cannot curate the data to harness its power. Further, uses for the blockchain are secure communication channels for applications with PKIs (Alsahli *et al*., 2021) (see 1.2.1 Permissioned vs Permissionless). Finally, blockchain can be a layer to anonymise identities and preserve privacy. Privacy preservation in the blockchain is achievable via the appliance of numerous techniques like encryption, private contract, anonymisation, mixing, and differential privacy (Hassan *et al*., 2019). For example, users can generate an identifier in intervals to remain anonymous to the rest of the network. Another case is the transmission to trigger only when a patient is tested positive (Marotta *et al*., 2021).

Although blockchain might add value to contact tracing apps, previous research has concluded that blockchain was unsuitable for contact tracing apps (Platt *et al*., 2021) early in the COVID-19 pandemic. However, this was early in the pandemic, and new development has been added since. The technology and proposed solutions may have matured since this review. In theory, many of the key characteristics that blockchain can offer would be valuable for contact tracing apps, such as mechanisms for data provenance, data immutability and, possible data tracking to ensure that the collected data only is used with the intention of contact tracing related to disease tracking.

### 2.1.3 Tracking COVID-19 Outbreak

During the pandemic, public health agencies and institutions have worked to obtain and aggregate timely COVID-19 case information to identify potential outbreaks and predict the spread of disease (Marbouh *et al*., 2020). Some government efforts had been hampered by the traditional information systems and the need for the appropriate protection of health information (Kritikos, 2020). As an example, the Human Medicines Committee of the European Medicines Agency requested the pooling and sharing of research resources for COVID-19 treatments with a broad reach to stakeholders to support information sharing (European Medicines Agency, 2020). While blockchain-based solutions are in the exploration phase to address public health needs, several blockchain solutions were introduced to promote near-real-time data sharing in a secure, decentralised manner, with three examples provided below.

The WHO launched **MiPasa**[25] as a global-scale communication and visualisation system to detect COVID-19 outbreaks and hotspots. MiPasa is an open data consortium with partners IBM, Oracle, Swisscom, Microsoft, and government agencies that utilise HACERA blockchain technology (MiPasa, 2021). While MiPasa can be exploited for a wide range of collaborative purposes, this technology is particularly valuable for sharing COVID-19 carriers and hotspots to characterise epidemiological data. Data are aggregated from public health organisations, while identities are protected with anonymous digital identifiers (Vervoort, Guetter & Peters, 2021). The blockchain-connected visualisation tools create insight for research and public health efforts to control the spread and containment initiatives (Marbouh *et al.*, 2020).

The **Public Health Blockchain Consortium**[26] (PHBC) represents health authorities and healthcare providers with several blockchain-based technologies to address COVID-19 communication and safety. The consortium offers a Critical Equipment Blockchain[27] to connect manufacturing facilities to ensure reliable supply chains for personal protective equipment, ventilators, sanitisers, test kits, and other medical equipment. **PHBCalerts**[28] is a vendor alert blockchain that records hospital reports for vendors and resolves incident reports. Hospitals and clinics can access this resource at no charge to review the reliability of vendor products and services. PHBC also offers **Virusblockchain**[29] to provide systematic infection status of communities and workplaces using validated reports of infection and contamination.

The **Coronavirus Data Hub** is possibly the largest government-level blockchain-based platform to aggregate and report COVID-19 information. The US Department of Health and Human Services implemented HHS Protect[30] to receive and aggregate COVID-19 data from 6,200 hospitals to track cases, ventilators, hospital beds, laboratory testing, and nursing home data (Brett, 2020). The blockchain creates a hash and provides a timestamped record for data parsing and curation to attest data as accurate and traceable. Further, HHS selected blockchain to share data in near-real-time within government agencies and provide aggregate information for public trust and transparency (Brett, 2020).

While blockchain technologies offer potential opportunities to address COVID-19 outbreak tracking, it is critical to consider that for blockchain-based application to demonstrate added value to a public health emergency context, "it should make extensive use of its encryption characteristics combined with decentralised peer-to-peer engagement so as to improve security, regulatory compliance, durability, consensus, selective privacy and timing" (Kritikos, 2020).

### 2.1.4 Blockchain-Based Federated Learning

The use of predictive models during the pandemic played a vital role in determining the strategy to safeguard public health. Predictive models were applied to forecast the trajectory of the infection's trend line and indicate peculiar cases that may need to be isolated in advance. Data are imperative in training models, and the training process calls for different data sources to produce a robust model that is representative of the actual model. In other words, cross-border collaborations for data exchange and data from multiple individuals are part of the social environment aspects. For example, efforts are made on data handling in a federated data consortium

[25] MiPasa - Analytics reDeFined. Source.
[26] PHBC - Public Health Blockchain Consortium. Source.
[27] Critical Equipment Blockchain (CEB) - PHBC. Source.
[28] Hospital Vendor Alerts- PHBC. Source.
[29] VirusBlockchain. Source.
[30] HHS Protect Public Data Hub. Source.

that is the fundamental structure for a predictive model. The World Economic Forum documented the eight steps for achieving a model on sharing sensitive health data in a consortium in a report.[31]

As data are a cornerstone, there are considerations to be taken into account. The underlying data are health data and, in extension, can be considered personal data. Despite the pandemic and the harsh situation, privacy is imperative to be held in this procedure to preserve individuals' right to privacy. The privacy fact and the need for collaboration of numerous entities suggested **federated learning** (FL) as a means for collaborative learning. The idea of FL is to construct a global model from locally trained models, allowing the exchange of models without transferring the datasets.

While FL can provide solutions in privacy, the collaborative model training can pose new threats. In the federated learning architecture, blockchain can be deployed to support activities and mitigate threats. The "trustless" environment that blockchain cultivates between stakeholders with conflicting interests fits the collaborative training environment. Blockchain can act as a common layer for the stakeholders in federated learning to enhance interoperability. Furthermore, data protection in blockchain can help in alleviating threats relevant to data alteration. Finally, the single point of failure prevention in blockchain can be integral in the harsh environment that calls for uninterrupted services.

There are suggestions in the architectural approach for deploying federated learning in a blockchain-based environment. The works like Ouyang *et al*. (2021) and Lo *et al*. (2021) discuss a framework for the early warning for COVID-19 and a trustworthy COVID-19 detection on X-rays, respectively. The framework proposed by Ouyang *et al*. (2021) uses blockchain and deploys its functionalities through smart contracts. The architectural approach foresees four roles to serve the framework, including federation members, social monitors, verifiers, and miners. As data stored in social partners' databases are expected to interact with the blockchain, the use of an oracle is vital to bridge these datasets with the blockchain for smart contracts execution.

Lo *et al*. (2021) use blockchain for achieving fairness and accountability in the federated learning environment. The components included in the architecture are minimal and retain the most vital ones: the central server that kick-starts the procedure, client, blockchain, and data-model registry. Similarly, Kumar et al. (2021) suggest a federated learning architecture with blockchain for COVID-19 detection in images. The work foresees two processes on the transactional data that are sharing and retrieval processes. These processes, along with the on-chain stored data, can potentially support network monitoring. The relevant data stored on-chain with a transaction has to indicate the timestamp, the type of transaction, the unique identifier of the one providing or requesting, and finally, the data.

## 2.2 USE OF VERIFIABLE CREDENTIALS IN COVID-19 PANDEMIC

The use and application of **verifiable credentials** (VCs) enable the **sharing of data between different entities** in a verifiable manner and according to the predisposition of the users or owners of the same credentials. One of the main benefits of verifiable credentials is giving users control of their data through self-management of credentials. The following section explains the application of VCs in the healthcare sector. Verified credentials are a generalisation of PKI (see 1.2 BLOCKCHAIN APPLICATIONS FOR HEALTHCARE DATA & TRANSPARENCY) in a decentralised setting that allows multiple authorities to issue credentials

[31] World Economic Forum. (July 2020). Sharing Sensitive Health Data in a Federated Data Consortium Model: An eight-step guide. Source.

according to an agreed-upon standard. In this section, a set of possible applications of the VCs in healthcare will be discussed.

The application of verifiable credentials brings benefits to the entities that manage them. The issuers and verifiers of the VCs also benefit from its use. In the case of issuers, the issuance of verifiable credentials allows them to ignore managing this information to verify it against third parties. In the case of verifiers, they are provided with a means to verify the information required. This shows the potential use of VCs is broad and covers a large variety of use cases in healthcare, as these types of solutions facilitate the presentation of information in a truthful way. Furthermore, the focus will be on the application of VCs to respond to some of the challenges mentioned in 1.1 CHALLENGES IN THE HEALTHCARE INDUSTRY and outline the most presumable use cases.

Verifiable credentials could be applied to manage and verify clinically validated clinical processes. VCs could serve as a means of certifying processes that third parties may use. For example, it would be possible to apply VCs for the certification of procedures in production processes and techniques with clinical application and capacitation of professionals, which will support resource optimisation.[32] This would ensure that every entity knows the validity of these processes, not replicating efforts, which also applies to the product traceability process (Ashkar *et al*., 2021).

Trusted collaboration between entities is another challenge and a requirement at the same time to be facilitated to satisfy. Being able to know and verify with full guarantee the capacities of the entities through their credentials issued by the competent authorities would facilitate such work.[33] This could even be improved by certifying the employees of these entities.[34] [35] On the other hand, data sharing is another of today's challenges. Data sharing is crucial to improve artificial intelligence (AI) algorithms. Nowadays, the data sources that are taken to train algorithms are different. Each entity manages its data and the corresponding data set against which the algorithms are trained. However, if these entities share and combine their data sets, the algorithm could be trained against larger data sets.

Accreditation of data sets worked to perform different experiments that would allow the sharing of verifiable data. Due to this, we could improve the training and optimisation of the algorithms mentioned above. Finally, the coordination of the different health units and entities is another of the main challenges mentioned. For instance, VCs for a patient's clinical history will facilitate interoperability between the various systems. In this case, the verifiable credentials would be applied to the users themselves to access their clinical history (Chadwick *et al*., 2019). The use cases mentioned are just a few examples of applications with verifiable credentials in the healthcare industry.

Driven by the situation generated by the pandemic, the use of VCs for the different procedures related to COVID-19 and its consequences is one of the contexts in which the existence of more initiatives is known (Lemmon, 2021). This is why the presentation of initiatives focuses on the use case of the context generated by COVID-19 and the corresponding initiatives to apply verifiable credentials that have emerged in this regard. Furthermore, we familiarise the reader with the known initiatives that propose the use of verifiable credentials or plan to use VCs to respond to the pandemic needs. Some of these initiatives have been implemented, and

[32] Dock. Verifiable credential use cases: Healthcare credentials. Source.
[33] Verifiable: Medical Credentialing & Provider Network Software. Source.
[34] Verified Credentials. Healthcare. Source.
[35] Health Tech World. 2021, 20 August). How decentralised identity & verifiable credentials will transform the world of healthcare. Source.

other initiatives represent associations and initiatives that promote the definition of a model that allows interoperability between the different solutions implemented.

**Good Health Pass Collaborative**[36]: The Good Health Pass Collaborative is an initiative that aims to define an interoperability model between solutions that seek to respond to the consequences generated by COVID-19. This initiative was initiated due to the mobility restrictions aiming to promote a model that would allow tourism to be promoted. Twenty-five leading companies and organisations are collaborating from the technology, health, and travel sectors, including Airports Council International, Commons Project Foundation, COVID-19 Credentials Initiative, Evernym, Hyperledger, IBM, International Chamber of Commerce, LACChain, Linux Foundation Public Health, Lumedic, Mastercard, Trust Over IP Foundation and others.

Although the focus has been on supporting vaccine management systems in some countries, the initiative is committed to being a public health tool. The Good Health Pass Collaborative was defined with several principles, including privacy and data security, user control, consent, trust, open standards, interoperability, among others.[37] For this purpose, the Interoperability Working Group for Good Health Pass has published a document, *The Good Health Pass Interoperability Blueprint*, that specifies the requirements to be met for the interoperability of these systems. This document focuses on using a decentralised identity architecture, incorporating Verifiable Credentials that comply with the World Wide Web Consortium (W3C) standard.

**Smart Health Card**[38]: SMART Health Card is a project born from the Vaccination Credential Initiative (VCI) in the United States and based on the W3C Verifiable Credentials. Currently, they are developing a framework that allows the issuance of verifiable credentials with the use of QR codes. Within the SMART Health Cards application, it is possible to use the credentials issued by the different health authorities. The Smart Health Cards are the signed verifiable credentials. These VCs must be signed by an issuer. In this way, any user who receives a credential from an issuer can access Smart Health Cards. Issuer management is executed through the CommonTrust Network, and every issuer is known. Based on this, a trust framework is built to manage health credentials. Anyone can do the verification of credentials with the use of the application. The development of these applications must comply with the Smart Health Cards framework specification. For example, it will be possible to correctly validate users' verifiable credentials on their Smart Health Card.

**EU Digital COVID Certificate** (EUDCC): EUDCC, previously known as the EU Digital Green Certificates (DGC), has been established to support freedom of movement in the European Union. However, each member state is administratively organised differently and has its own IT resources. This is one of the reasons the European Union has defined the minimum requirements that the EUDCC must meet to enable interoperability between these systems and the consequent mobility of citizens. However, before the announcement of the European Union, there have been several initiatives presented and valued by different administrations. Among them, we have some related to Digital Identity and Verifiable Credentials, which had begun to be implemented. For example, in countries like Cape Verde and Germany. These Digital Identity initiatives seek to respond to the problem of interoperability based on the implementation of the so-called Self-Sovereign Identity (SSI).

The EUDCC certifies that the person has been vaccinated against the SARS-CoV-2 virus, has overcome the disease, or has a recent active infection test (PCR or antigen test) with a negative result to support them to move freely in the European Union. At this stage, there are no plans to make use of verifiable credentials or

[36] Good Health Pass. Source.
[37] Good Health Pass. Principles. Source.
[38] SMART. What is a SMART Health card? Source.

SSI, even if some elements were initially considered for implementation in the "Interoperability of health certificates Trust framework".[39]

**LACPass**[40]: LACPass is a multinational project for implementing digital vaccination certificates for the countries of Latin America and the Caribbean. Within this project, the international interoperability standards that are being defined by the World Health Organization (WHO) are agreed upon and adopted by the countries participating in the project. This project will leverage the LACChain blockchain infrastructure. LACPass aims to guarantee interoperability and exchange of clinical care summary in LAC countries. It will seek to improve the exchange of clinical care information on patients between different actors and levels of the health systems at the national level and promote it at the regional level.

**Lanzarote Covid Safe**[41]: Lanzarote Covid Safe is a pioneering and innovative pilot project, which has been promoted by the Cabildo de Lanzarote and developed by Alastria, King's College London, IN2, and Continuam. The pilot lasted four days and included 60 participating tourists who have stayed at the Hotel Meliá Salinas and have carried out a "complete tourist programme", including visits to tourist centres, restaurants, excursions, and use of private transport. A blockchain application was developed to inform tourists about the COVID-19 protocols and services. The pilot has complied with the measures registered and traced the Alastria blockchain network (red-T). Tourists and third parties (e.g., administrations, compliance companies) could access information on COVID-19 prevention measures. AENOR is the pilot project reviewer to certify compliance with the COVID-19 safety protocols to guarantee the response and resilience capabilities of the solution. The Meliá chain, the Biolab laboratory, Cicar (car rental), and the Lanzarote Art, Culture, and Tourism Centers have collaborated in this test. In addition, the safe tourist experience model can be applied to all activities in the sector.

The Lanzarote Covid Safe pilot project has been carried out by implementing the SSI concept. In the pilot, the Alastria Blockchain network (red-T) has played the recipient of verifiable credentials. When a user had a negative result in the corresponding test, the operators of the origin airport (Heathrow) registered the credential in the blockchain network, then sent a message with a URL to the user to download the credential. In this way, when a user landed at the destination airport (Lanzarote), the user could download their credential. In the process of downloading, the user had to verify the signature of the VC, carrying out a check against the Universal Resolver of the Trust Framework of the Blockchain Network. Once a Verification Operator at the destination airport asked the user to show their credential, they could present their VCs. Like the Verifier Operator in the airport, any other verifier could confirm the credential given by the user, making the corresponding inquiries against the Alastria Blockchain network.

**NHA Card**[42]: NHA Card is the digital certificate of Cape Verde that safely stores all kinds of health certificates. It collects clinical data on the country's inhabitants and visitors, unifying the documents for all the administrations in a single system. It has been made in the European blockchain network of Alastria and its Alastria ID, which complies with all European digital identity standards. In turn, there will be an integration with the data exchange platform of the Government of Cape Verde, which aims to speed up and optimise processes and significantly reduce the time and administrative workload of this type of procedure. The implementation

[39] eHealth Network. (2021). Interoperability of health certificates: Trust framework. Source.
[40] RASCEL. LACPass - Regional Digital Vaccination Certificate. Source.
[41] King's College London. (2021, 08 June). KCL TEST piloted in Lanzarote. Source.
[42] NHA Card - COVID Certificate from Cape Verde. Source.

aims to guarantee and control information use and cybersecurity exchange through this interoperability platform.

**Scudo Platform**[43]: Scudo is a system that facilitates the inviolable unification of individual data, based on digital identity, capable of uniting health data in a one-person way (wallet) and a secure manner that each individual can have this information on their smartphone. The system is compatible with any other system approved by the European Union, such as EU Digital COVID Certificate. Using blockchain technology, the health entity certifies that a citizen has received the vaccines or carried out the PCR (Polymerase Chain Reaction) or antigen tests. Using their wallet, they can present these credentials to authorised validating bodies, such as at the airport, theatre, football stadium, or a restaurant, among many other places. This solution embodies the idea that each person decides with whom they want to share the credentials generated by the health administration whenever it makes the electronic "wallet" available.

[43] Scudo presentation video. Source.

# CHAPTER 3. REGULATORY, PRIVACY & ETHICAL IMPLICATIONS

The theoretical and innovative underpinnings of blockchain and related technologies that can be useful within the healthcare industry have been studied for nearly half a century (Lamport, Shostak, & Pease, 1982; Hamming, 1950). However, problems arise when attempting to implement solutions due to several reasons, starting from shortage of personnel within the medical industry with a deep understanding of the different underlying technologies to the lack of readily available modular software components that increases the time to bring a viable solution to market.

In the following chapter, we address three primary concerns that limit the practicality of blockchain within the healthcare industry, namely **data integrity and accuracy, regulatory and privacy considerations**, and **ethical implications**.

## 3.1 HEALTH DATA ACCURACY

In theory, blockchain technologies can provide capabilities for health data accuracy and integrity. Wong, Bhattacharya, and Butte (2019) suggest that regulators would "need only check blockchain hash string equivalence" (p. 6), which would also reduce a regulator's burden (Hirano *et al*., 2020). When using a blockchain, Omar *et al*. (2020) propose that "mistakes or malicious attempts do not occur since the recorded data is validated using consensus algorithms" (p. 15). The hope is that blockchain would somehow improve health data accuracy (Wu & Tsai, 2018).

However, a blockchain does not guarantee **data quality**, as there are many points of **data vulnerability**. Possibly the most significant impediment to data quality is referred to as "the first-mile problem" (Alles & Gray, 2020). The "first mile" involves the time and activities until data are added to an electronic system and represents the possible difference between reality and the data captured (Alles & Gray, 2020). Specifically, a blockchain cannot prevent human measurement errors or misunderstandings (Wong, Bhattacharya, and Butte, 2019), fraud or impersonation (Hirano *et al*., 2020), or even data entry errors such as entering information for the wrong patient (Learney, 2019). Health information is notoriously inaccurate. When Vezyridis & Timmons (2021) examined National Health Services data in the United Kingdom for prospective use in research, they noted significant inconsistencies in original data entry. In general, these inconsistencies might be caused by several factors, from a human error to data integrity (Zozus *et al.,* 2015). For example, Vezyridis & Timmons (2021) noted that diagnostic codes for the same diseases varied significantly from one clinic to another.

In many ways, health data quality is still subject to the consideration of "garbage in, garbage out" (Learney, 2019), and any inaccuracies would be carried forward in a blockchain (Wong, Bhattacharya, and Butte, 2019). While the goal is for a blockchain to serve as a source of trusted data, LaPointe and Fishbane (2019) point out that we have not achieved "trusted data" by adding inaccurate data to a blockchain.

## 3.2 REGULATORY CONSIDERATIONS

The paramount regulatory considerations for blockchain in healthcare involve interpretations and uncertainties regarding the degree to which blockchain technologies can meet the letter and spirit of **GDPR**. GDPR was designed to protect EU residents' personal data but also to promote economic and social progress within a framework of security and justice (GDPR, Recitals 1 and 2). To support these aims, blockchain technology brings the potential of participatory governance to balance transparency and security (Chassang, 2017), aligning with GDPR's focus on democracy of data management (European Economic and Social Committee, 2019, n. 4, par. 1.1).

In theory, the privacy objectives of GDPR would also be aligned with core principles of healthcare, as health information is categorised as "sensitive personal data" subjected to higher levels of protection (GDPR, Article 9). Blockchain technologies feature mechanisms that can ensure secure transmissions and data encryption to safeguard patients' rights to privacy (European Economic and Social Committee, 2019, n. 4, par. 1.1). The European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains, as amended in 2020, describes four potential benefits of blockchain for healthcare (European Parliament, 2020). The Parliament had recognised the potential of distributed ledger technologies to improve data efficiencies for data exchange and interoperability with a focus on identity verification (n. 13) and under more patient control (n. 12 and 14). The European Parliament stresses the importance of protecting sensitive health data (n. 14). This resolution calls on the Commission to "explore DLT-based use-cases in the management of healthcare systems, and to identify benchmark cases and requirements that enable high-quality data entry and interoperability between different DLTs" (European Parliament, 2020, n. 15).

Technological innovations and the global distribution of blockchain nodes have created **new uncertainties** for protecting and sharing health information. First, GDPR grants individuals the right to have data amended (GDPR, Article 16) and the right to be forgotten (GDPR, Article 17). Therefore, it is uncertain the degree to which health information must be deleted from a practically immutable blockchain ledger (Evangelatos, Özdemir & Brand, 2020). Several technological solutions have been suggested for addressing data deletion on a blockchain, including chain pruning, obfuscation, or the addition of smart contracts that prevent access (Herian, 2020). However, it is unclear which methods would be acceptable to the European Commission.

Blockchain also emphasises the **importance of trust** among individuals and organisations, theoretically enabling and enhancing health information sharing (European Commission, 2020, n. 4). Blockchain facilitates trust through disintermediation and transparency (European Economic and Social Committee, 2019, n. 4, par. 3.16). However, lack of trust is a major contributing factor in why healthcare organisations have not shared health data at a sufficient scale (European Commission, 2020, n. 4). It is unknown whether the introduction of blockchain would change healthcare organisations' data-sharing approaches. In addition, while blockchain-based transparency is promoted as a method for increasing trust, there are stringent GDPR limitations about the nature and levels of access to personal data. As a specific example, Centro Hospitalar Barreiro Montijo in Portugal was fined EUR 400,000 for GDPR violations related to insufficient access controls and inadequate protections for the confidentiality of health information (Monteiro, 2019). Instead, it may be more feasible to track access to health information using a blockchain. For example, the Estonian eHealth Foundation applies a layer of blockchain to track and facilitate access permissions for health data stored in the electronic health record system (Priisalu & Ottis, 2017). Compliance staff periodically view the audit trail to ensure that access was legitimate and limited to authorised healthcare personnel (Bell *et al*., 2018).

Blockchain technologies are regularly touted for creating transactions that are theoretically "pseudonymous." In the GDPR, Articles 4(5) and Recitals 26 and 28 describe "pseudonymisation" as the processing of personal data so that the data can no longer be attributed to specific data subjects (with additional conditions to separate information that could link to an identifiable natural person). On a blockchain, an individual's transactions are associated with specific alphanumeric key pairs that don't directly identify an individual but are (presumably) unique and often described as pseudonymous (Leon-Sanz, 2019). Calvaresi *et al*. (2019) add that blockchains track and link transactions to users by design. In addition, as a data privacy mechanism, a blockchain may store the hash or the encrypted personal data (Chassang, 2017). While the GDPR does not regulate the processing of anonymous data, there is no clear distinction between anonymous and pseudonymous health data. GDPR Recital 35 specifies that data concerning health include "a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes" and it is unclear if blockchain-based keys could constitute pseudonymous data requiring protection as personal data (Mondschein & Monda,

2019). Therefore, EU legislators and regulators are asked to provide interpretation regarding blockchain-based processing of data concerning health and whether core blockchain data would necessitate data protections.

The committee generating this report is aware that EU authorities have been alerted to confusion surrounding the interpretations of GDPR and blockchain (European Parliament, 2020) and that there have been calls for revisions to GDPR (European Economic and Social Committee, 2019). Specifically, the European Economic and Social Committee (2019) acknowledged that GDPR was drafted when blockchain technologies were largely unknown, and GDPR must be periodically reviewed with consideration of emerging technologies and data risks (n. 4, par. 4.2). While the *European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains* recognised the potential benefits of blockchain technologies for healthcare, the resolution emphasised that blockchain technologies must currently be compatible with GDPR. The resolution recommended that the European Commission and European Data Protection Supervisor provide clarification regarding the circumstances where data protections are warranted when using distributed ledger technologies.

As mentioned above and in previous work (Shuaib *et al*., 2021; Hasselgren *et al*., 2020), there are several inherited compliance issues with blockchain and GDPR, especially for public blockchains, such as Article 24 Responsibility of the controller and Article 17 Right to Erasure ('right to be forgotten'). These are, however, issues that are not limited to the healthcare domain but face most blockchains solutions by default and possible other decentralised technologies. Although most of the GDPR requirements can be addressed with proper blockchain architecture, there are several grey areas where compliance is questionable (for example, two articles listed above). As a result, there is no GDPR compliance blockchain out of the box, but there are GDPR compliant blockchain solutions for healthcare (Hasselgren *et al*., 2020).

The European Commission is advised that outdated privacy regulations could hinder the adoption and acceptance of blockchain technologies for healthcare (Allen *et al*., 2020). In addition, **legislators and regulators have a critical role** in encouraging blockchain healthcare innovations in the EU and will enable progress with more explicit direction.

## 3.3 ETHICAL CONSIDERATIONS

Blockchain transitions from its infant stage, and more and more solutions adopt the technology in numerous sectors. As the technology adoption increases, the potential consequences and moral aspects should be investigated (Tang *et al*., 2019). Essentially, blockchain technologies designed for healthcare create nuanced ethical considerations. Blockchain platforms offer design features that generate unique economic and privacy incentives, and healthcare stakeholders need to understand **cross-sector relationships and influences** (Allen *et al*., 2020).

Incorporating ethical considerations in the planning and design phases is referred to as "**ethics by design**" (Brall, Schröder-Bäck & Maeckelberghe, 2019). Ethics approaches exceed the requirements for regulatory compliance to engender meaningful respect for individuals and place individuals' preferences as a primary consideration (Charles & Magtanong, 2022). To determine appropriate ethical design features for healthcare blockchains, it is valuable to review ethical design frameworks. Ethical design frameworks often list ethical principles, organisational values, risk mitigation strategies, and privacy/security sustainability (LaPointe & Fishbane, 2019; Allen *et al*., 2020). Organisations can utilise existing documents for inspiration, such as the Government Blockchain Association's blockchain ethical design framework for healthcare (Allen *et al*., 2020), or create their own around a moral core of respecting the interests and rights of the individuals impacted by their technologies (Edenberg & Jones, 2019). An organisation's values are then embedded in the technology's design and programming, such as including specific features or methods to improve access and accessibility

(Allen *et al*., 2020). Compliance features should also be designed into the technology, and regulations would govern the use (Allen *et al*., 2020).

EU legislators and regulators are encouraged to review ethical design frameworks for healthcare blockchains to make **informed decisions** about the impact of blockchains on the healthcare ecosystem. Without consideration of ethical approaches, leaders may lack understanding regarding how blockchain technologies will address specific healthcare goals (McQuinn & Castro, 2019). Allen *et al*. (2020) recommend the development of scenario-based ethical dilemmas across blockchain uses in various healthcare and value chain scenarios to ensure that the right questions are considered for decision making. LaPointe and Fishbane (2019) add that these ethical considerations should be holistic to integrating all blockchain attributes with human behaviours. Overall, ethical frameworks will enable legislators and regulators to embed ethical approaches to regulatory, legal, operational, and financial decisions about healthcare blockchains.

Blockchain is a general-purpose technology that interacts with other technologies and fields like big data, cloud computing, and AI. The **interactions between technologies augment the complexity** of the ecosystem analysis, as each application can have different subjects for ethics. For example, the healthcare supply chain runs the ethical issue of zero-state for accuracy (Tang *et al.*, 2019). This issue is relevant to every application in the supply chain. Essentially, blockchain is appropriate to track the provenance throughout the supply chain. Still, the risk lies in the initial transaction where data are introduced for the first time on the chain.

Another ethical issue included in the literature is the **individual's privacy**, specifically in the scope of GDPR's right to be forgotten. GDPR is a regulation aiming to safeguard users from the illicit use of their data, so ethical issues are blended with regulations. Blockchain is a technology that uses an add-only ledger making data deletion impossible. As healthcare applications apply blockchain, they have to deal with this ethical issue. A European project, **MyHealthMyData**, suggests a blockchain model that adheres to the regulation and covers some privacy concerns (Bayle *et al*., 2018).

As the blockchain has different uses in healthcare, this report finds it appropriate to focus on ethical subjects with blockchain and AI, as AI and blockchain is one of the promising technology synergies, as we found through the survey results presented earlier (see 1.5 OPPORTUNITIES AND CHALLENGES: EXPERT OPINION). Moreover, the fact that federated learning gained traction during the pandemic is an indication of a trend for training models in a collaborative fashion. Finally, the concern of algocracy, meaning to decide based on algorithms, is a subject of discussion. Hence, to facilitate the development of ethical guidelines for the blockchain when **applied with AI**, we focus on already established guidelines and recommendations in the context of AI.

### 3.3.1 Ethics-by-Design in AI Solutions for Healthcare

> *"Nevertheless, the problem of meandering is certain to re-emerge once we learn how to make machines that examine themselves to formulate their own new problems. Questioning one's own "top-level" goals always reveals the paradox-oscillation of ultimate purpose. How could one decide that a goal is worthwhile – unless one already knew what it is that is worthwhile? How could one decide when a question is properly answered – unless one knows how to answer that question itself? Parents dread such problems and enjoin kids to not take them seriously. We learn to suppress those lines of thoughts, to "not even think about them" and to dismiss the most important of all as nonsensical, viz. the joke "Life is like a bridge." "In what way?" "How should I know?" Such questions lie beyond the shores of sense and in the end it is Evolution, not Reason, that decides who remains to ask them."*

These are some of the questions Prof. Marvin Minsky raised back in the 1980s.[44] Still, the high speed of evolution of technologies aiming to become cognitively autonomous makes them more pertinent than ever before.

Over the past years and more recently, a lot has been researched and written on AI and the implications of its use and purpose of use on many aspects of our daily lives. Due to its importance and the complexity of issues, as well as the severe consequences that errors may have (even loss of human life), the healthcare sector lends itself for an in-depth evaluation of the impact that the purpose of and the use of AI systems can have and how an "ethics-by-design" approach can be conceived, adapted and applied so that the most worthwhile purpose is easily and clearly identified and the maximum benefits of its use are attained.

What is considered an ultimate purpose for using AI systems in the healthcare sector? Who will define if this purpose is worthwhile, and how can such a notion of "worthwhileness" be embedded in an AI system? How could the "worthwhileness" of the purpose of use be expressed in an "ethics-by-design" model of AI in healthcare applications? Who will examine that the embedded process is indeed an "ethics-by-design" one? Who will monitor and ensure compliance with ethics notions? Whose ethics notions will need to be embedded, and how to reach a consensus? How can technology developers "bypass" the limits of their knowledge and own beliefs to develop a system that can be characterised as "objective" or "common sense"? In other words, how can we remove bias, and if this is not possible, how can we ring-fence it at least? What are the gaps in the interaction between the various actors, tech developers, users, Social Science and Humanities scientists, regulators, policy, and decision-makers? How can we enable the dialogue between the various actors?

Starting from a more philosophical question: What is the ultimate purpose of the use of AI in healthcare and how can we be sure that this is worthwhile for the cause-and-effect analysis and the interaction between different "agents"? Also, how can we ensure that the AI solution deployed, and answers provided are the right ones? Add to the analysis the explanation of "why" the AI system chose the specific solution to verify the correctness of the answer. Top everything with the potential existence of bias in inputting the information to the AI system choosing the solution. It becomes evident that the plexus of aspects factoring in the analysis and feasibility of an AI "ethics-by-design" for healthcare applications and use is a challenging question. Should the objective no longer be a negation? Should it be Do Good rather than Do No Harm?

But is it possible to achieve a Do Good only AI? An AI that encapsulates "ethics-by-design" and not only from the bench but from its conception to market? How can ethics and technology "marry" to ensure a Do Good only AI? An AI that will enable all involved stakeholders from concept designers to developers and users to Do Well by Doing Good!, meaning allowing the stakeholders responsible for the technology conception, design, and development to maintain and increase financial benefits while the users will be maintaining and expanding the benefits derived from the deployment and use of AI technologies in the healthcare sector.

A transdisciplinary approach and collaboration are necessary, combing knowledge and experience from Science, Technology, Engineering & Mathematics (STEM) and Social Science and Humanities (SSH) disciplines. It is also recommended that learnings and practices from the theory of '**design thinking**' are integrated into the conception and design phases of AI systems. Design thinking is based, among others, on the principle that empathy is embedded in the design phase with the users for whom the innovation is developed to understand their pains and problems fully. The latter, in turn, is converted to the **human-centred design** that focuses on understanding the perception, the needs, and expectations of the person who are

[44] AI memo No. 603. November 1980. Published in Minsky, Marvin, "Jokes and their Relation to the Cognitive Unconscious." Source.

looking for a solution to a specific problem and whether the proposed solution has been designed in a way to and will effectively and efficiently resolve the problem for which it was designed. Human-centred design can be further enriched by **value sensitive design** (VSD) principles, which is a method that embeds values into a technical design.

As proposed in an analysis published at the beginning of 2021 by Steven Umbrello & Ibo van de Poel (2021), VSD could be integrated into AI systems design to address the challenges posed by the need for transparency, explicability, and accountability of AI systems as well as those posed by machine learning (ML) which may lead to AI systems adapting in ways that "disembody" the values embedded in them. For this purpose, they proposed a threefold modified VSD approach: (1) integration of a set of VSD principles (AI4SG) as design norms facilitating more specific design requirements, (2) distinction between the values promoted and respected by design ensuring outcomes that not only do no harm but also do good, and (3) extension of the VSD process aiming to encompass life cycle of an AI technology to monitor unintended value consequences and redesign as needed (Umbrello & van de Poel, 2021). They elaborated on this approach, building further on the outcomes of AI for Social Good (AI4SG) projects, and they used as reference the case of a SARS-CoV-2 contact tracing app.

How can a regulatory or standards framework address such an "ethics-by-design" approach from conception to market to ensure compliance control, due diligence, monitoring and benchmarking, while demonstrating the necessary adaptability due to the rapid evolutions in AI technologies?

To identify an appropriate regulatory framework, the US Food and Drug Administration (US FDA) issued in April 2019, a proposal for a review framework for artificial intelligence-based medical devices. The idea behind the US FDA's proposed framework was to enable the use of AI/ML Software as Medical Device (SaMD), prioritising patient safety. The FDA described a Predetermined Change Control Plan in premarket submissions as part of this proposed framework. This plan would include the anticipated modifications, referred to as the SaMD Pre-Specifications[45], and the developed methodology to implement those changes in a controlled manner to manage risks to patients[46]. It proposed measures and approaches to monitor algorithm changes and ensure that these are implemented according to pre-specified performance objectives and change protocols, referred to as the Algorithm Change Protocol, apply a validation process to improve the performance, safety, and effectiveness of AI/ML software, and include real-world monitoring of performance[47]. In this way, the US FDA intended to support the technology development and the technology developers while ensuring the maximum benefit for the users.

In addition to describing the framework, the discussion paper asked for stakeholder feedback[48]. In January 2021, the US FDA published the Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan as a response to the stakeholders' feedback on the discussion paper. They took into consideration public health needs to facilitate innovation through AI/ML-based medical software while providing appropriate oversight for it. This was in line with the mission of the newly launched Digital Health Center of Excellence[45]. In October 2021, The US Food and Drug Administration (FDA), Health Canada, and the United Kingdom's Medicines and Healthcare products Regulatory Agency (MHRA) jointly identified 10

[45] The Pew Charitable Trusts. (2021, 5 August). How FDA Regulates Artificial Intelligence in Medical Products. Source.
[46] HoganLovells. (2021, 15 January). Five highlights from FDA's new AI device regulation Action Plan. Source.
[47] U.S. Food & Drug Administration. Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML) Based Software as a Medical Device (SaMD). Source.
[48] U.S. Food & Drug Administration. (2021). Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan. Source.

guiding principles that can inform the development of Good Machine Learning Practice (GMLP) for medical device development.[49] These guiding principles aim to help promote safe, effective, and high-quality medical devices that use AI and ML.

In June 2021, the WHO published guidance on **Ethics and Governance of Artificial Intelligence for Health** identifying six core principles. These are (1) protection of autonomy; (2) promotion of human well-being, human safety, and the public interest; (3) ensuring of transparency, explainability and intelligibility; (4) fostering responsibility and accountability; (5) ensuring inclusiveness and equity; (6) promoting AI that is responsive and sustainable (World Health Organisation, 2021).

Due to the large amounts of data needed to utilise AI, one of the challenges of AI testing is the fact that most model test scenarios are not equipped to identify human bias. This bias is often integrated into the training of AI systems and in the testing of the input datasets. And this is where the aspect of Prof. Pearl's writing in the *Book of Why*[50] comes into focus: the knowledge. The knowledge that is input at the conception phase by the technology or algorithm developer, which is, as stated by Prof. Pearl as well,[48] limited by default to the amount of information that the technology/algorithm developer disposes of at the specific point in time plus by their own personal beliefs and experiences. How can we then be sure that an AI system can objectively guarantee maximum results? How can we detect the 'blind spots' to address them and avoid a 'Garbage-in-Garbage-out' (GIGO) effect? Have the questions about which data have been omitted and why been asked? Perhaps it is necessary to train the developer and/or prepare the trainer in an 'applied ethics' approach? If this is the case, on which standards should this training be based? This situation requires an increased awareness of how human bias can affect AI processes and dictates the need for the proper exercise of the system developers and system testers.

Furthermore, reference in different writings on AI systems is made to "**common-sense reasoning**". AI systems do not dispose of common-sense reasoning. Consequently, the question that is posed is whether it is feasible, desirable or necessary to develop an AI system with applications in healthcare with a common-sense reasoning capacity. If this is the case, how could this be achieved? The integration of a transdisciplinary ethical due diligence approach and an ethics impact assessment methodology for AI systems used in healthcare could solve this problem where decisions assisted by AI systems can be represented in a common-sense manner. However, as long as the decisions are robust, traceable, explainable, trustworthy and inclusive without this meaning that AI systems dispose of common sense in an intrinsic manner as long as the decisions are robust, traceable, explainable, trustworthy and inclusive.

As is the case of reinforcement learning, a reward-based solely training process is not sufficient. Applying the same principles of pedagogy, an AI system needs to develop a sense of responsibility, accountability and consequences of its choices and actions, especially those leading to a harmful result, worst-case scenario, loss of human life. Is such an AI system realistically achievable or even desirable? One can argue that such a system could be desirable for assisting humans with decision-making, but how could we achieve such an "ethical by design" system?

[49] U.S. Food & Drug Administration. (2021, October). Good Machine Learning Practice for Medical Device Development: Guiding Principles. Source.
[50] Pearl, J., & Mackenzie, D. (2018). The book of why: the new science of cause and effect. Basic books.

## 3.4 REGULATIONS, PRIVACY AND ETHICS THROUGH THE EYES OF A LAWYER: INTERVIEW WITH NENAD GEORGIEV, PRIVACY AND TECHNOLOGY LAWYER

**Expert profile: Nenad Georgiev** is a privacy, cyber and technology lawyer with experience in all facets of privacy, cybersecurity and data protection compliance for emerging technologies, including blockchain. His background is in industry, government, and academia. He holds a master's degree in Information and Communication Technology Law with specialisation in privacy and cybersecurity from the University of Oslo and a master's degree in European law from the University of Nottingham. In the past two years, Mr. Georgiev acted as Regulatory, Legal and Data Privacy Co-Lead and Legal and Ethical Manager in the PharmaLedger project. Currently, he is working as **Data Protection Manager** at **Nordic Entertainment Group** in Sweden.

### 3.4.1 Insights from Legal Practice

**Q1: From your legal practice experience as a lawyer, what are the most common requests or questions from your customers you receive concerning blockchain in healthcare? Generally, are such requests a common practice?**

**A1:** I would like to state from the beginning that the present regulatory environment in healthcare is a complex system with many levels of compliance to contend with. With the introduction of the GDPR in 2018, maintaining compliance programs in this industry became even more challenging. Since its implementation, this data protection regulation has been a pressing concern for those operating in the digital economy and beyond because non-compliance may result in hefty penalties and economic losses.

Unfortunately, privacy is still an afterthought in the software life cycle when it comes to digital solutions. However, many people are coming to realise that once a system is fully developed, privacy cannot be completely addressed in a simple and straightforward manner. I have witnessed a positive shift in the engineering mindset, with systems being designed from the bottom up to respect privacy. I am particularly encouraged by the increased interest in involving privacy specialists early in creating solutions. This is especially true for blockchain-based solutions because the bulk of inquiries I receive from blockchain developers and managers care about **GDPR compliance** or **governance matters**.

**Q2: You mentioned governance issues. Could you give a couple of examples?**

**A2:** Setting up an adequate governance framework is a critical step in developing any blockchain network. Due to blockchain's decentralised character, many stakeholders may be involved in its operation. Unlike single server settings, where it is relatively easy to pinpoint the responsible party when, for example, an incident occurs, there is usually no single owner of blockchain infrastructure. This necessitates a governance mechanism to address the questions of responsibilities and accountability. As a result, when you have a network with numerous parties engaged, the contractual arrangements become more complicated, especially as new ecosystems evolve and blockchains are being built up of multiple layers.

Different governance options may be more appropriate than others depending on the use case, the blockchain network, and its intended deployment. From a legal standpoint, establishing a single legal entity with decision-making power over network development, updates and failures may be the most straightforward governance

approach. This concept, however, contradicts the *raison d'être* of blockchain, which is to move power and decision-making from a centralised body to a distributed network. When everything is managed by a single entity, in principle, there is a risk of discouraging trust in the processes. Therefore, the question of governance must carefully be examined and appropriately adapted to support both effective functioning and compliance efforts.

**Q3: Nowadays, the opportunities using blockchain in general and in healthcare are well understood and considered promising. Yet, what are the key legal issues in terms of healthcare applications using blockchain?**

**A3:** Many of the legal issues surrounding blockchain implementations are not unique to healthcare use cases, but they may be compounded by the health sector's critical nature. If I were to list them, **data protection** would undoubtedly be one of this sector's most pressing legal concerns. Data circulating within healthcare is to a considerable extent sensitive, necessitating greater protection. In this context, the principles of medical confidentiality, in addition to privacy beyond data protection, are extremely important. Blockchain-based applications may bring about risks associated with patient visibility and monitoring, as well as the creation of aggregated profiles of patients when the blockchain system combines data from multiple sources. Data breaches in the health industry – I'm referring here to both **purposeful** and **accidental disclosure** of health and medical information – can have serious human rights ramifications because they can subject patients to stigma and discrimination in addition to other harms caused by a privacy violation. With the introduction of new regulations all over the world in recent years, not just in Europe, we have seen the evolution of data privacy and security standards. Thus, privacy is the primary legal and ethical consideration to keep in mind while designing, deploying, and maintaining a blockchain-based healthcare solution.

**Jurisdiction** is another important legal concern that pertains to blockchains in general but is especially critical for their use in healthcare. Geographic boundaries for jurisdictions exist, but the distributed nature of blockchains allows them to circumvent these boundaries since a network may theoretically be maintained by nodes located worldwide. In this case, two legal considerations are relevant. First, the potential cross-jurisdictional nature of a blockchain network may **necessitate compliance** with an overwhelming array of legal and regulatory systems. National legislation and the organisation of health systems can vary greatly between countries, making compliance with all applicable legal obligations cumbersome. Second, there must be **legal certainty** on the law to be applied in the event of aberrant behaviour. As a result, the allocation of responsibility and liability among all relevant stakeholders must be carefully reviewed as part of the governance structure to ensure that patients' rights are guaranteed.

### 3.4.2 GDPR Compliance

**Q4: You also mentioned GDPR. When we studied the existing blockchain solutions in production, we noticed that mostly the developers state full compliance to the regulations despite some evident challenges [to be fully compliant]. But when you examine their solutions more closely, many prefer not to discuss the compliance matter to a larger extent. Why do you think this is the case?**

**A4:** We live in one of the most disruptive eras in technological history, with numerous emerging technologies redefining and revolutionising how our society operates. Blockchain as a technology is still immature. Over the

previous decade, we have seen how the technology has expanded well beyond its original application in cryptocurrency, with new applications spanning the healthcare and pharmaceutical industries, among the rest. As with any emerging technology, various legal, social, technical, and political struggles must be overcome or removed before the technology can be widely used and fully integrated into our society. Addressing the initial flaws and underlying problems that are perceived as barriers to adoption necessitates either incremental improvements or fresh breakthrough advances.

In the case of blockchains, the GDPR has been portrayed as one of the major impediments to their adoption. When you come across an impediment on your path, you normally take steps to overcome it. And this is exactly what we are witnessing with blockchain's advancement. You might call it a trend, but I would say it is a general direction toward which the technology is veering, with the result being an increasing number of blockchain-based solutions that claim to have made tweaks to comply with the GDPR. And I expect this tendency to continue as the technology evolves and blockchain developers work on overcoming the hurdles posed by privacy laws.

However, I have noticed a frequent misconception among the community that there is such thing as full compliance or partial compliance. Legally, the issue is rather binary: you are either compliant with a certain law or not. Incorporating privacy and data protection into the technical design protocol of a blockchain-based solution does not guarantee compliance if the technology is later deployed and utilised in a way that contradicts the privacy and data protection principles. Although privacy-preserving functionality supports compliance efforts, it does not exclude the rest of the environment from GDPR scrutiny, owing to the fact that technology is not independent of the community in which it functions. So, to claim that a particular solution is GDPR compliant, a more holistic strategy with accountability measures, safeguards, and processes is required.

**Q5: As an end-user, a patient, what can I do if I suspect my rights are violated? One example is the "right to be forgotten".**

**A5:** Generally speaking, the primary duty for monitoring the application of the GDPR falls with the relevant national Data Protection Authority (DPA) – there is at least one in each EU Member State. If you believe your data protection rights have not been effectively enforced, you have several remedies. You can lodge a complaint with your national DPA, which will investigate the matter and look into the specifics of, for example, your request to have your data erased, any legal justifications for the controller to refuse erasure if your request was handled in a timely manner, and so on. Based on this, the DPA will contact you within three months to notify you of the status and outcome of your complaint. If you are not satisfied with the decision or think your case has been mishandled, you can bring an action directly before a court against the DPA. Taking legal action in court against the organisation or company that you believe has breached your data protection rights is also an option. I am not aware of any such examples in the blockchain context, although the DPAs are receiving a growing number of complaints in general. This has both positive and negative aspects. Even though it is encouraging to see that the public is becoming more aware of their privacy rights, an increase in the number of complaints may indicate that organisations and businesses are not exercising their due diligence when it comes to GDPR compliance.

**Q6: What are your views on privacy matters, and how should privacy be addressed as regards blockchain-based solutions applied in the field of healthcare?**

**A6:** When talking about GDPR compliance, it is important to remember that the GDPR, which is a technologically agnostic legal framework for personal data protection, refers to the requirement to put in place appropriate technical and organisational measures to address the risks that a specific processing activity poses to our rights and freedoms. However, there is no one-size-fits-all legal response to compliance. Rather, conformity with these data protection requirements must be evaluated using a **risk-based approach**, considering the specific context in which the blockchain-based application is intended for deployment.

Having said that, the risk of a privacy violation can be considerably reduced, for example, by minimising or limiting the probability or likelihood that threat actors will be able to identify the person behind the data on the ledger. In a blockchain system, there are several techniques or controls that may be used to support GDPR compliance efforts:

- Keeping as much **personal data off-chain** as possible, with off-chain data connected to the ledger solely by a hash value. Moving personal data, particularly sensitive data, off-chain to a segregated data storage is closely related to data minimisation because it keeps data out of the hands of various threat actors and alleviates some of the concerns raised about individuals' rights to have their personal data rectified or erased as guaranteed by the GDPR. When personal data is successfully erased from off-chain storage, it is best practice to do an anonymity assessment on the residual hash to ensure that identifiability is beyond the bounds of possibility.
- The second matter to consider is implementing **access control** and establishing a robust **governance framework** to limit network access while allowing only trusted members only to have the ability to add data on the ledger. This reduces the number of threat actors and their affordance or capacity to enact privacy violations.
- Finally, it is necessary to set up contractual relationships as part of the governance structure, ensure compliance with the GDPR accountability principle, and implement **privacy-preserving features** in the design of the blockchain protocol to the greatest extent possible.

### 3.4.3 Benefits of Blockchain Applied in Healthcare & Pharma

**Q7: Do you think blockchain applied in healthcare or pharma brings any benefits from a legal and ethical perspective? If yes, what are these benefits? If no, then why?**

**A7:** Many processes in healthcare and life sciences can benefit from blockchain-enabled solutions, which are ripe for innovation owing to several data-related matters, such as interoperability, transparency, privacy, and security, among others. Combining healthcare and technology creates previously unimaginable opportunities. Nonetheless, we must carefully examine them while keeping in mind current limitations since there is still a lot of hype around the potential of blockchain in these ecosystems. As a result, its capabilities may be overstated at times, which is why it is vital to identify where blockchain may offer value in healthcare and focus on specific use cases to prepare them for integration into our society. I am mostly talking about **medical and pharmaceutical supply chain management**, **self-sovereign identity management**, **patient consent and access permissions for health data sharing**, **and clinical trials management**.

From a legal standpoint, the benefits of these applications can be measured by whether they support achieving the desired policy outcomes for which certain laws and other types of regulation have been enacted. Accountability is a central purpose of law and a tenet of ethics. Many of the previously mentioned use cases can help streamline regulatory review and approval processes while also improving patient safety. Falsified

medicines, for example, are a growing threat, and we can prevent them from entering the legal supply chain and reaching patients by exploiting blockchain features to **improve the verification process**.

Another example is that leveraging blockchain for **data access** matters allows data subjects to have greater control over their data and digital identity - objectives pursued by the GDPR and data protection law in general. Much of the data in healthcare is held in silos. When blockchain is applied in **combination with other technologies** in the health information system, it can allow patients to access and review their health information, grant authorisations to users and disclosures of their data, and revoke permissions to share it with third parties. **Individual autonomy** is a fundamental moral principle, and there are several projects underway to use blockchain for self-sovereign identity management. In the case of clinical trials, using blockchain technology to capture and bind participants' consent to any version of the study protocol enables tamper-proof recording of when and what the participants consented to, **improving protocol adherence** and **transparency** in potential regulatory and ethical violations.

These are only a handful of the benefits of blockchain, and as the technology evolves and adoption expands, more advantages may emerge. In my opinion, however, those are the areas where we should concentrate our efforts. The supply chain is widely recognised as a practical application in which the benefits of blockchain are fully realised and required. And we can see how using blockchain for **identity verification**, and **patient access permissions to health data sharing** may provide important advantages.

### 3.4.4 Ethical Strategy and Ethics by Design

**Q8: The legal and ethical framework might differ based on the particular use case. So, when selecting blockchain technology, is there any tailoring mechanism to particular technology to respect legal and/or ethical matters as with a specific healthcare field or domain?**

**A8:** Indeed, as digitalisation spreads through healthcare, appropriate legal, regulatory, and technical standards are required to support and facilitate digital activities. In general, healthcare is heavily regulated, and the legal environment may vary depending on the use case at hand and the location of the blockchain-based solution's implementation. Regarding the EU's legal and regulatory framework for blockchain, we see legislative initiatives in cryptocurrency assets but not yet in healthcare. However, a **pan-European blockchain regulatory sandbox** is being prepared, with use cases to be tested in a range of industries, including health. As a result, legislative proposals to promote the development and implementation of this technology in key areas such as healthcare may emerge. This leads us to believe that some type of guidance is on the way.

Concerning ethics, I am not aware of any standard **ethical strategy** for designing, developing, and deploying a blockchain platform for healthcare use cases. But what we are witnessing with emerging technologies is a push for **ethics by design** approach. **Ethical guidelines** have already been created and published for solutions that raise substantial ethical concerns, such as AI. Because a blockchain does not operate in a vacuum, domain experts can get inspired by those guidelines and appropriately incorporate the ethical concepts of autonomy, justice, beneficence, and non-maleficence in the solution architecture by reviewing and adapting the design based on the solution's aims, operation, and target audience.

**Q9: Who do you think should bring insights into ethics by design, awareness of legal, ethical, and privacy matters to the team? Do you consider there should always be a specialised lawyer in the team, or could other members play this role?**

**A9:** In my opinion, it is the project management responsibility to bring in an expert, who does not have to be a lawyer, but who is well-versed in and **understands the legal and ethical issues** and can alert everyone on the team that these are matters that should be considered from the outset of technology development. This is the proper approach to build and sustain a solution, not because of the threat of penalties for non-compliance, but because it is the correct way forward. At the end of the day, we must create solutions that are respectful of everyone's rights and liberties, are not discriminatory, and do not cause harm to marginalised groups of our society. And it is for this reason I believe regulators, policymakers, and other concerned stakeholders should be issuing guidance aimed at increasing public understanding of the legal and ethical issues surrounding emerging technologies.

### 3.4.5 Recommendations to Developers and Regulators

**Q10: What would you recommend (or note as a key message) for a community to ensure success when working with blockchain technology in terms of legal, ethical, and privacy matters?**

**A10:** My first recommendation is directed at developers because they are usually the first line of defence when building a solution respectful of the rules already in place. I strongly advise technical experts to keep legal and ethical issues in mind throughout the entire process of the development process. Why is this important? When you are confident that the legal and ethical considerations are underwritten into the solution's design, you **create trust**. As such, adoption becomes considerably easier and more predictable.

Keeping the concept of privacy as forethought and adopting a privacy-by-design methodology allows for measurability and compliance with the privacy laws and regulations. If I were to break down my recommendations depending on the maturity level of a solution, I would advise those designing a system or working on scoping the concept on **understanding the legal requirements** and formally **document them** in a software requirement specification. For those deploying a solution, I recommend reviewing and confirming that you have a **plan and policy in place** for ongoing **maintenance** and patching, as well as continuous evaluation of threats and vulnerabilities. They should conduct an external and internal audit to document compliance with the applicable laws and regulations before final deployment occurs.

Recent history taught us a significant lesson that regulators and policymakers need to adopt a more agile and responsive approach to regulation to maximise innovation. In the case of blockchain, this would imply taking the remaining necessary steps in the form of regulatory guidance to address the community's **privacy and other legal concerns**. Such a strategy would not only provide legal certainty but would also allow regulators to proactively shape technology trends. Emerging technology should be seen as a work-in-progress, with adequate leeway for it to grow while also interfering, when necessary, with regulatory guidance and/or industry standards to steer its progress in a path that benefits our society and protects our citizens.

Finally, but certainly not least, it is necessary to ensure **diversity**. Having worked at PharmaLedger, I noted that the diversity of the skillset of the team was critical in bringing value to the table and ensuring progress in

the solutions' development from several viewpoints, including ethical and legal. Furthermore, the consortium's diversity, which is represented not only by business process owners, technical experts, and managers but also patient representatives' organisations, hospitals, and social science stakeholders, was vital in creating innovative approaches to address the patients' needs. Therefore, tackling the regulatory issues posed by emerging technologies necessitates a multilateral and pragmatic strategy that brings developers, regulators, policymakers, and civil society together to achieve a common objective.

# CHAPTER 4. BUILDING FOR THE FUTURE: PRACTICAL VIEW

## 4.1 PRACTICAL VS THEORETICAL APPLICATIONS OF BLOCKCHAIN IN HEALTHCARE: INTERVIEW WITH ROBERT CHU, CEO OF EMBLEEMA

**Expert profile: Robert Chu** is the **co-founder and CEO** of **Embleema**, based in the United States. Before establishing Embleema, Robert worked for IQVIA, an influential healthcare services and technology company performing clinical trials as a contract research organisation; healthcare data then is sold for life sciences for drug development and assessment of efficiency and safety of the drugs. At IQVIA, Robert ran the Global Technology Group, focusing on software, data collection, data packaging, and analytics in healthcare applications.

### 4.1.1 Embleema

**Q1: Could you tell us about your decision to launch Embleema?**

**A1:** My background was in the healthcare sector, but not specifically on the blockchain. In essence, I was not familiar with blockchain before founding **Embleema**[51]. The perspective for launching Embleema was more of a business one rather than a technology one. The main drive for Embleema came in my time in IQVIA, where my work included interactions with numerous stakeholders like pharmaceuticals, governments, healthcare professionals, hospitals. We were working with every stakeholder in the healthcare sector except patients. That was disturbing **because no data could exist without patients**. You should not set patients aside since improving patients' health is the very reason we are all working in healthcare. That is my profound belief, along with my team members.

Even more vital is that patients must benefit from their data directly. And this is new in terms of the healthcare data marketplace and clinical trial marketplace. Currently, the traditional model considers patients just as a data source without getting any return for their data. The main and undeniable argument is that the return is a life-saving drug. The data generated out of the clinical trial are the sole purpose of it. But the clinical trials data do not get back to the patients and benefit them.

Another problem with the data comes from the **privacy perspective**. Patients have a greater need for understanding how their data is being used with incidents like Facebook's data used for election manipulation. There is a growing consciousness in the United States regarding understanding the actual uses of patients' data and ensuring there are no illegal or unethical uses. I am confident that European citizens have a broader consciousness because of GDPR.

Apart from monitoring for illegal activities, patients desire to document the range of processes on the data to determine if they agree with them. Patients do not want their data to be used against their beliefs or without their prior authorisation. That is the core vision in Embleema. We aim to do it in the right fashion, meaning the creation of a trusted framework for patients in terms of data collection and usage at every step of the process.

[51] Embleema website. Source.

A **trusted framework is vital** for establishing a new healthcare data model and making it faster, more ethical, and more efficient. Currently, the main issue with healthcare data is that these are proprietary datasets. The data belong to entities like hospitals, pharmaceuticals, and others. As a result, clinical trials cannot run on existing data because owners of existing data do not want to share it. Therefore, the healthcare data cost is extremely high, translating directly into high drug costs. For example, we see this in medications involving complex datasets like genomic datasets to produce personalised or precision medicines. As a result, these drugs become extremely expensive, meaning hundreds of thousands of dollars per patient per year, because generating data is slow, inefficient, and costly. The clinical trials that gather and analyse all this data using very poor technology require significant manual interventions, increasing the cost.

Our aim is to flip the model upside down and give the data ownership back to their source - the patients. A trusted framework **centred around patients** allows **data reusability**. The reusability of data in healthcare is very new. Data can be reused by having patients allow access to the data to the different research entities. This is a simple concept, but it diminishes costs with significant benefits for patients and the industry. Data re-usage sets the floor for more efficiency, reduced costs, and speeding up the development of new drugs. This is the vision and benefits that we have built as key design points for our solution.

**Q2: Could you tell us briefly about your solution and how you store the data?**

**A2:** One of our key software components is **HIVE**, an **off-chain enterprise database** storing clinical and real-world healthcare data. The most exciting thing about HIVE is that the FDA [Food and Drug Administration] has a license from us to use HIVE. They use it for their regulatory decisions for new health products involving big genomics datasets or other complex datasets. HIVE is obviously an utmost secure, and privacy-enforced platform as FDA deals with data from clinical trials that are extremely sensitive. For example, the public can panic if a data leak shows controversial details on a new COVID-19 drug. The FDA has a complex security system to avoid such scenarios: HIVE has passed NIST 800 [National Institute of Standards and Technology] certification and has the regulatory Authorisation to Operate (ATO), a very stringent certification process that takes years to obtain.

While developing HIVE, we followed **international standards**, namely FHIR [Fast Healthcare Interoperability Resources], ICD-10 [International Classification of Diseases], disease ontologies that define the amount of data and the variables, and as I mentioned, we comply with the FDA standards.

Blockchain is open by essence, as anybody in the network can access the stored information on the chain, and there are security issues to account for data on the chain. So, it can be challenging to keep personal information on-chain, even encrypted data. I believe that storing healthcare data on-chain is dangerous, so we opted for off-chain storage for healthcare. In our case, all the data are stored in our HIVE database. Our blockchain stores two types of information: a de-identified patient consent and an audit trail of changes for each data element in HIVE (also de-identified). Once an algorithm requests access to particular data elements, HIVE checks against the blockchain for consent and authorisations against the data elements, a given number of algorithms can have permission to access data. The access can be denied with no data leaving from or being analysed in HIVE. I think we are one of a few people who enforce the **compliance of the patient's consent technologically**.

In our solution, first, we store the consent number on a blockchain with the data on the study ID the data is being shared with, the subject data perimeter allowed for access, the duration of the access right, and other

information characterising the consent. The extension can happen if the patient re-consented, which requires updating the corresponding field for the duration. In essence, two separate transactions are stored on the blockchain: one transaction is about the initial consent form, and a second transaction is an update from the re-consent form.

To summarise, we have **no identifiable data on the blockchain**. The on-chain data can be patient ID, subject ID, consent ID, study ID, and data element ID. All these data are metadata that do not reveal the underlying information. It is possible to erase all personal information from HIVE, so there would not be any future procedures on that information. Erasing information on the blockchain is impossible due to the nature of the technology. That is why only de-identified information is included in the transactions. The ledger only stores transactional data without any patient data. Metadata of the actual data are part of the transaction, and the metadata does not allow to recompute the original data element. But Europe is hesitant to this architecture and solely focuses on the deletion part for the right to be forgotten rather than others means that it equally protects patient privacy, if not more.

**Q3: How do you use blockchain in your solution?**

**A3:** These are the two main things that we do with blockchain. One is for enforcing a true voluntary, explicit consent to share data. It is common to collect consent from patients in the normal process of care. The example is in the case of surgery where patients admitted to hospitals sign consents forms. There are cases where consent forms include standard terms like the involved risks, but terms about the data are inserted somewhere in the middle with sometimes very difficult legal language not easily understandable for people that are not lawyers. These terms on the data generally set hospitals as the data owners and make patients abolish their claims. This is a problem because we are talking about the case of **forced consent**, where patients, if they want to access care, must agree to any of those terms. Patients have no other option; they need to have the surgery for their own good, and they sign. It is contrary to **informed voluntary consent**. Hopefully, GDPR should change those practices, but this is where we are coming from.

The next issue with consent is also concerning: the patient's consent can be signed on a piece of paper or electronically signed and stored, but there is no automatic link between the consent storage and the processes applied to the data, like sharing and any research on these data. There is no easy and irrefutable way a data processor can guarantee a patient that his data has not been misused.

A data analyst must intervene and work on determining the processes applied to the data by investigating the database. The process is manual as there is no technology enforcement. Moreover, the manual process needs the data user's goodwill since this check is time-consuming and can take months. We apply blockchain to solve this problem. Basically, we link the data and the backend procedures like data analytics. Blockchain acts much like a "police officer", prohibiting the data exchange or data views to unauthorised uses.

Another key point of blockchain is **data provenance**. The notion of provenance for healthcare data comes from a regulatory standpoint of view. Our biggest customer is the FDA [Food and Drug Administration], which works on the approval of new drugs and medical devices. A new drug's process begins with a life sciences company developing a new drug, running clinical trials, and finally submitting the data to the FDA. These procedures will showcase the drug's effectiveness on a particular disease, and there is no danger for patients. FDA is obligated to scrutinise the data deeply to be reassured that the data is not fake and scientifically relevant. FDA is also very stringent with the notion of provenance. FDA can request proof that any specific

data elements defined by date, patient, or doctor have not been unduly changed. The pharma company must be able to prove this at any time.

The data lifecycle is long and complex as the data are generated, stored, processed, and finally delivered to the FDA. Provenance is information that needs to be trusted, very much like consent, and it is an appropriate use case for blockchain, in our opinion. Once the data are collected, we regard that moment as the "birth time" and store this moment on the blockchain to track further data transformations. Data tracing becomes easy and quick as all we need to do is press a button to publish the accurate and trusted report. That is highly valuable for the drug approval process and the regulatory use case.

**Q4: Is it possible to join your network?**

**A4:** Embleema operates a **permissioned**, **private network**. As of today, all the nodes run in-house, which means that no external entity can join the network. The reason for that is we wanted to be able to run a stable network before letting external partners run additional nodes. Theoretically, patients may be concerned about Embleema tampering with the blockchain as the company holds all the nodes. But in fact, we see that patients appreciate a lot what we are doing to protect their privacy and to empower them with their data, so there is no immediate requirement for decentralisation of the network. We are doing something entirely different compared to other solutions. Patients can provide their re-consent, check the data, and are secure with the blockchain that enforces consent. While patients are not experts in the blockchain, they understand the benefits and the security offered by this technology. Decentralisation is not a core and immediate requirement. As it is not a primary requirement, there is room to take small steps in deploying external nodes in a reliable way. But it is in our longer-vision plan to **decentralise the network as part of building trust** in the blockchain network.

There are two aspects to consider in terms of decentralisation: the **technology supplier** and the **governance**. Embleema is the technology supplier of the system. The governance involves policymaking with the ability of multiple healthcare stakeholders, with patients first and foremost, to make decisions. In our opinion, governance should involve stakeholders from the whole range of the healthcare sector like patients, regulators, government, doctors, pharmacies, hospitals, managers, and each life science industry should be represented in the network to represent the voice of these industries. For instance, pharma companies access data for developing new drugs, while hospitals' aim to reduce operational costs. This is why open participation and including every representative as the ultimate goal of each group is different.

### 4.1.2 Data Protection & Regulations

**Q5: Based on your working experience in Europe and the United States, would you give us your perspective on the specifics in regulations for data protection?**

**A5:** In the States [USA], the main regulation around protecting health data is called HIPAA [Health Insurance Portability and Accountability Act]. There are obvious differences in this regulation compared to the GDPR. The first one is that entities auto-certify their HIPAA: there is no need to be certified before going live. Once a data breach occurs, this event gets the breaching entity into trouble. In contrast, Europe requires compliance before any occurring incident. While European regulation includes exceptions, the discussion with the French privacy agency showcased to us the need to have a dossier to be approved before the deployment.

The main concept in sharing data is clear: **data must be de-identified** in the US with no possibility of re-identifying them. However, the situation becomes challenging once only a few patients participate in the dataset. In this example, it may be impossible for any method to completely de-identify the data. Should we then forbid any research for rare diseases, even if patients agree to share identified data? In our opinion, it should not. This example demonstrates well that there needs to be a **balance between privacy and innovation**. What is not productive is an extreme position in either privacy or innovation at all costs.

There are similar procedures in Europe, like data anonymisation and pseudo-anonymisation methods. Europe goes one step further with GDPR, which is great. We feel that blockchain is an exceptional tool to enforce GDPR. The audit trail that is produced with blockchain is part of the GDPR. Then, informed consent is another subject in GDPR that is possible to achieve with blockchain.

An unclear piece in GDPR that can result in hurdles is the right to erase one's data, namely the right to be forgotten. In our case, we delete data from the off-chain HIVE to satisfy this right. A trace of data is kept proving that the data existed at some point in time. However, there are complexities if data are simply deleted since FDA [Food and Drug Administration] can utter their concerns about the providence being broken. Data deletion in the blockchain is impossible. Blockchain has multiple uses to enforce GDPR as it is tamper-proof and can trace transactions. However, once some asks to erase their data, all the other benefits are left on the side, and blockchain suddenly becomes unusable. Some legislation may lag the updates in technologies, so there might be **room for updates in legislation** as technologies mature and grow. Again, we should find reasonable solutions here rather than stay rooted in a too extreme position.

### 4.1.3 Success Factors & Recommendations

**Q6: What were some challenges that you encountered during the development? Was there one that was most difficult to address?**

**A6:** The biggest **challenge** is to bring blockchain to an **enterprise production** level. In our view, it is easy to create a proof of concept and deploy nodes and smart contracts in a few weeks. But being enterprise-grade is something different coming from my years of experience in IQVIA and IBM. Enterprise-grade involves certain attributes and has nothing to do with functionality. Functionality is easy to achieve in the blockchain.

The first thing in enterprise-grade is to have a scalable solution where the response time is reasonable, considering more and more patients join the network. Moreover, the response time must be consistent, so response time estimates should be accurate regardless of the day, time, and workload. Services have to run constantly and smoothly, meaning to operate 24/7. Finally, capacity planning is an important factor for enterprise-grade solutions. For example, a given study with 700 patients will call for a data analysis that requires computational power, so the solution must have **enough CPU** [central processing unit] and other resources for the task.

Today, we have close to zero tools to evaluate these factors to produce an enterprise-grade. So, it is necessary to allocate resources: time, people, and money, to build these tools in-house for performance, predictability, and capacity planning. As an example, it is common in blockchain for a node to lag some blocks, and it is vital to detect such nodes in any network, which mandates writing scripts for procedures to detect these nodes and potentially slow down the rest of the network. That is only one case, but more cases call for developing tools to guarantee an enterprise-grade level of service.

Achieving enterprise grade is the biggest challenge by far. Transactions in the banking system are executed in a matter of seconds to secure the monetary exchanges with a **99.9999% reliability**. The big technology companies have a business advantage as they have amassed experience and built this kind of tools. So, we probably need many years working with the blockchain to get to that level.

**Q7: The industry is interested in Embleema. How did you achieve success? Is it a matter of good social skills, a drive to find appropriate collaborators, funding?**

**A7:** The **success** comes from signing contracts with **big customers** such as the FDA and delivering a quality product. To achieve this, there should be a system in production that works reliably, is reusable, based on customisation rather than coding, and produces consistent results for different clients' use cases. To date, we are running many use cases with our same platform and blockchain spanning from regulatory bioinformatics to high-quality to multi-modal real-world data and evidence.

What actually helps to develop a solution is **taking one small step at a time**. It is challenging to foresee and account for all the difficulties you are to meet while developing. The step-by-step approach is pragmatic and results in a product being developed. For example, decentralisation is a central point of using the blockchain, but in reality, it might not be an ultimate priority as there are constraints to adhere to first, like reliability and performance.

**Q8: What technical or other skills will you be looking for in a candidate in the blockchain sector (maybe a developer or a manager)?**

**A8:** It is vital that we share the same belief that connects and drives the team. After that, there is a little bit of everything as the requirements for the solution vary. For example, some people are technically savvy, while others are scientifically oriented. As patients are our most important stakeholders, we take special care in great design for our app's **UI/UX** [user interface and experience]. Nevertheless, the fundamental is a **common belief** to serve patients and improve healthcare that guides the team efforts.

At Embleema, we are a small team, but the team's core consists of a **very experienced group** of people. The experience comes from different places and expertise. So, it is far better to have a small group with the right and deep expertise, a true willingness to work together, and a genuine motivation to improve healthcare.

**Q9: Do you feel the regulations can aid in developing blockchain solutions? Or perhaps it is the opposite, slow down the innovation?**

**A9:** The right to be forgotten is a topic that comes to my mind. **No solution is perfect**, and existing issues should be measured. In my opinion, blockchain has 99% benefits accompanied by 1% of issues stemming from deletion impossibility. **Innovations should not be blocked** as research is carried out to mitigate this 1%, and there are much greater benefits in the appliance of new technologies.

Europe seems to focus on a centralised system, where an authority (data processor) needs to be trusted to ensure user privacy. But blockchain is decentralised, and no such single authority exists, so perhaps regulators

in Europe, which are extremely smart, should be a little bit open to dialogue to get **feedback** and find a suitable solution for decentralised technologies. The feedback can be valuable as it comes from running use cases in the real world with a wealth of feedback from thousands of patients in our case. A diverse range of **opinions can shape regulations** that secure public welfare without blocking innovation.

## 4.2 FROM INNOVATION TO PRODUCTION IN BIG PHARMA: INTERVIEW WITH MARCO CUOMO, BLOCKCHAIN TECHNOLOGY EXPERT

**Expert profile: Marco Cuomo** is the **Blockchain Technology lead** at **Novartis Pharmaceuticals** and has worked for the company for the past 16 years. Prior to that, Marco worked in other areas such as finance, military service, and government. He has experience in multiple roles, initially starting as a software developer, and also worked as a system administrator & within project management. Since 2016, Marco has been working with blockchain technology and is currently a co-lead for the architectural workstream in the PharmaLedger project.

### 4.2.1 PharmaLedger

**Q1: Can you share a few words about the PharmaLedger project? What is the key technology in the project?**

**A1:** In 2016, Novartis was curious about the implementation and application of blockchain technology in the pharmaceutical industry. The team quickly realised that this was something that could not be achieved or accomplished independently. Other Pharma companies needed to align together in order to build a blockchain network and digital trust ecosystem across the industry.

Throughout our research, we came across the IMI Innovative Medicines Initiative [now rebranded as Innovative Health Initiative], which collectively joined pharmaceutical companies and public partners in a collaborative consortium. The **PharmaLedger**[52] project was born, allowing 12 global pharmaceutical companies and 17 public and private partners ranging from academic, legal, and technical entities. The idea was to build a platform for the healthcare industry and to make that platform usable, scalable, and tangible. We proposed use cases along the value chain for the industry, including **supply chain**, **clinical trials**, and **health data** (patient data).

Blockchain technology encapsulates principles of decentralisation, distributed consensus, immutability, and transparency. Our initial vision and thought process were that we would be completely agnostic to the chosen technology and protocol. However, an additional layer was required to achieve this solution. The multiple submissions for the project suggested different technologies, one of them being proposed was **OpenDSU**[53]. The DSU stands for '**Data Sharing Unit'**. At the time of submission, it was called **off-chain storage** that utilised secret smart contracts.

Back in 2018, it was unclear the impact that the chosen technology would have. However, it has become clear to the project that this piece of software/technology was needed to help create the platform for developers.

[52] PharmaLedger website. Source.
[53] OpenDSU homepage. Source.

From the beginning, we had the idea not to define a single blockchain technology for all participants to work with, as the idea of defining a sole blockchain technology sounded conflicting in a transparent and decentralised network. In other words, the project aim was to be blockchain technology/protocol agnostic, and for that, an in-between layer or abstract architecture was necessary (see Figure 4).

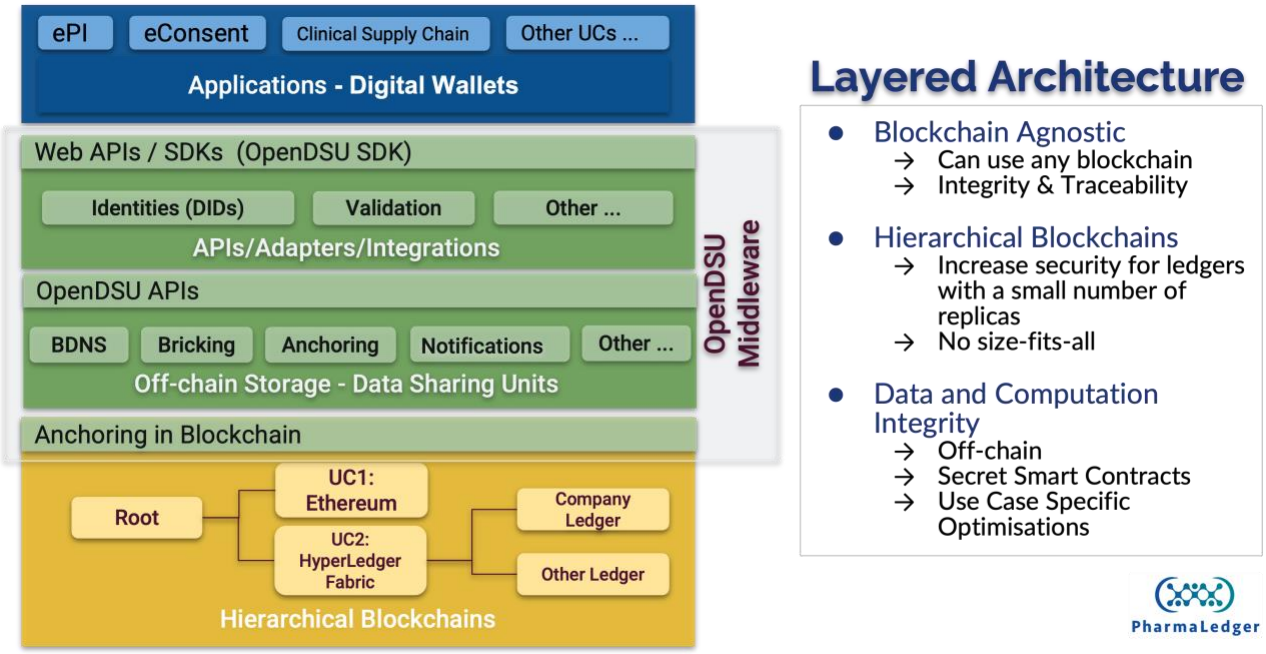


**Figure 4:** Layered high-level architecture of PharmaLedger

**Q2: What use cases do you have in the project and which do you think will benefit the most from the project and its technology?**

**A2:** PharmaLedger has developed **eight use cases**:

- Electronic Product Information
- Anti-Counterfeiting
- Finished Goods Traceability
- Clinical Supply Chain
- eConsent
- Clinical Trial Recruitment
- IoT
- Personalised Medicine

Given the cross-functional nature of the use cases, there was the possibility of merging some of them, such as eConsent, IoT, and Personalized Medicine.

The electronic product information (ePI) use case has the greatest potential as a business case overall and has benefitted the most from the project and OpenDSU technology. Alternative technologies compared to the blockchain can help in use case implementation and deployment, but decentralised applications have gained momentum and recognition as a solution that the pharmaceutical industry is interested in. This is because it

**drives patient engagement** and medical and healthcare **data empowerment**. Patients want to become more involved in controlling who has access to their personal information and how it is being used.

Another set of use cases with the most potential are those related to clinical trials, specifically regarding the **recruitment of patients** into trials. In the future, the automation and digitalisation of the whole drug development process will result in immense benefits on several fronts for pharma companies. The World Economic Forum referred to one benefit in a published paper in 2018 claiming that the development time can be reduced by 20%. On average, the drug development process can take approximately ten years to develop, considering the 4 phases of clinical trials that need to be conducted to bring a drug to market. A reduction to an eight-year development cycle would mean that patients could access the drug two years prior. At the same time, the pharma company can produce revenues from the drug sales earlier. Consequently, funds could be allocated to carry out more research and development. This is a **win-win scenario for patients and pharmaceutical companies**.

This process will not be realised overnight, but it is a slow and steady progression. Optimising drug development is a long journey as there are many different participants and stakeholders within the ecosystem. Convincing everyone to switch to a digital blockchain solution will take years, and PharmaLedger is pioneering this mission. The process becomes more complex because incumbents, like the CRO [contract research organisation], can regard digitalisation as a threat to eliminating intermediaries and deem some of their services obsolete.

**Q3: It seems that the project is ambitious and promising, aiming to bring technical or technology innovation into the industry. Do you think such transitions are common and why?**

**A3:** The PharmaLedger project differs from traditional approaches in pharma, as indicated by the level of engagement and collaboration and the range of project partners, including public organisations and institutes, SMEs [small and medium enterprise], universities, hospitals, patient organisations, and pharma companies. While the approach is different from the norm, the idea remains that the project's result should be incorporated in a productive or operational environment and commercially exploited in the future. This is something that we strive towards implementing in pharma companies. The implementation should exceed simply using or proving something; the **value proposition** that blockchain technology has to offer must be higher than this. This is why from the beginning of the project, we established a workstream focused on **sustainability and governance**. The project foresaw this workstream as a means to implement processes for the project's sustainability even after it is completed. That is different from projects where the results are finite once the project has come to an end.

I am not aware of many projects similar to PharmaLedger, as the majority are set up differently in the pharma industry. Some projects are vendor-driven, like IBM or SAP, where vendors convince one or two companies to build an initial prototype. After the initial prototype and implementation, these projects look for other partners to join the network. For example, Maersk and IBM collaborate in deploying the TradeLens platform. The issue is having the original partners as owners of the solution and the joining partners act as "followers" in a sense. Essentially, the original partners could dominate the project or product; hence it is centralised in nature. Similarly, start-ups can lead the projects instead of vendors, but the issue remains in overcoming the initial phase and moving towards a truly decentralised system in a larger ecosystem. This is what PharmaLedger wants to build, a **decentralised digital trust ecosystem** that is **blockchain technology-agnostic** utilising OpenDSU.

Pharmaledger started with 29 partners and managed to deliver something useful in the last two years despite the numerous partners. The implemented system is not perfect or fine-tuned, but a system for making difficult decisions exists. I believe that the project is one of the few that adopted this approach. One of the project's unique strengths is that the results will be **vendor-independent** with no vendor driving the development. Each partner is equally involved in the success of the project despite the allocation of resources.

### 4.2.2 OpenDSU & Off-Chain

**Q4: You've mentioned the OpenDSU technology. Would you tell us more about the technology in a nutshell?**

**A4:** Two things are important in understanding OpenDSU:

**The developer's perspective:** OpenDSU technology abstracts access to the blockchain. The abstraction allows developers to save time and focus on the functionality since access to the blockchain is expedited. A relevant comparison is the existence of website tools like frameworks that relieve website developers from starting something from scratch with only HTML, CSS, or JavaScript. That is why there are applications in React and Angular. With these tools, the developer's life becomes more manageable, simplifying their activities and work processes. There is no need for developers to stress over each device's different web browsers and versions. Even security activities are available in frameworks to work with. As a result of using frameworks, the developing phase is more efficient and accelerated as a result.

OpenDSU is similar to these frameworks. It helps developer's program and build regardless of the specific blockchain technology and relieves them from dealing with the technology specificity. That is one of the big advantages for developers, as it **abstracts the need to interact and develop independent blockchain languages**.

**The business perspective**: The other thing about OpenDSU is the business perspective, as it enhances security from the standard blockchain technology. Security covers confidentiality and privacy issues that are generally not the strongest topics for adopting blockchain technology. OpenDSU mitigates the issues in these aspects, as no patient, personal, or business data are stored on the blockchain. With not much technical information, **blockchain is used as a layer to anchor the off-chain data**.

In PharmaLedger, we plan to build a digital trust ecosystem and have blockchain and blockchain-based solutions as the backbone. We envisage that blockchain technology will only represent 10-20% of the final solution within the digital trust ecosystem. OpenDSU allows the building and collaboration of different use cases and applications to enable interoperability and cross-chain connectivity. Interoperability should permit leveraging the different applications and features possible with the OpenDSU framework application. For example, a developer can easily unite one DSU from one use case with another DSU from another. This is possible because it is the same technology, and we can use a single key to access and read the data.

Wallet features are required for accessing the blockchain for key management. While using OpenDSU as a layer, there is no need to develop another wallet for each use case. We can use a universal wallet to load the necessary data from several other wallets or solutions. OpenDSU is an open-source technology, and in PharmaLedger, we work on expanding the ecosystem based on the OpenDSU. And as I mentioned, OpenDSU

is not there to replace everything, but it intends to be an **abstraction layer** to the blockchain and benefit the application developers.

**Q5: The OpenDSU is the solution for off-chain data storage. So, why an off-chain framework?**

**A5:** Off-chain is important because the blockchain is not a typical database in the traditional sense where relational databases hold data. Blockchain can be inefficient in storing and managing data because its main characteristic is that it provides a layer of trust depending on the cryptographic function used. One must realise that blockchain technology is not a silver bullet in the sense that it may not be the one chosen technology to fix all problems. A simple database may suffice if the objective is to manage and control data. It really depends on the **problem that needs to be solved**.

One pertinent characteristic of blockchain technology is **how it captures immutable data**. And the goal of the business use cases that are intended to be implemented using blockchain is not to store the data on-chain but to manage assets and values. If data was stored on-chain, the solution would not be scalable. A real-world example comes from accounting, as ledgers are extensively used to track assets for entities. It is normal to document an asset in the ledger with minimal and vital information like its name and value. If someone needs more details on the asset, a binder holding more information should be referenced; but the detailed information is not part of the ledger. Also, storing data off-chain allows for more flexibility. The practical standpoint is that data on the blockchain has to be replicated on all the participating nodes, and this procedure should not take hours for practical reasons. For example, X-rays are pictures that can take up **gigabytes of memory**, and they have to be replicated in each node. Consequently, there are **privacy concerns**, as there should be reassurance for organisations and how they handle the data. The situation may change in the future, but off-chain data storage seems like a reasonable approach.

From another perspective, immutability for data means that the data is stored on the blockchain and cannot be altered. We need to define the purpose of blockchain; is blockchain a solution to store our data like pictures, or is there a better way? Blockchain can help in procedures where there is a need for timestamping documents and tracking supply chain information. The information stored on the distributed ledger is essential for many services, with **notary services** and **data provenance**.

Blockchain is ground-breaking due to the possibility of **building trust in a trustless environment**. There is an example of land registries, where trust is currently placed on institutions that follow appropriate and adequate methods. In the future, someone may not even have to trust the institution anymore as reliability is built due to the blockchain application. We need to consider events that can endanger the land registry documented in physical format and papers. For example, fires can destroy the registry, or malicious bad actors can manipulate the registry's data. Blockchain is a technology to guarantee that the data are not manipulated, but the **off-chain frameworks give the flexibility** for the data we store.

### 4.2.3 Identity Management

**Q6: Identity management is one of the most discussed topics when it comes to the large-scale adoption of blockchain solutions. So how do you deal with it in PharmaLedger?**

**A6:** We have our **Demiurge tool**. The tool is developed not to replace the digital or decentralised identities but to **manage the identities** within our OpenDSU-based use cases. Users always need an account, even for a simple task like opening a wallet. As a result, a DID [decentralised identifier] is essential to create an identification step for the users. Our new tool **simplifies DID creation** and operates within the OpenDSU world, but external DID's are still supported for the entities that join the ecosystem later. For instance, there is still the need to manage data for the blockchain solution and have an API [application programming interface] for distributing electronic product information. The Demiurge tool simplifies the administrator's tasks. Therefore, we consider incorporating the tool with the existing account management for a **single sign-on**.

Another issue is the identification of the entities on the blockchain. On that subject, the project consortium works with Glife and GS1, which operate with two different **credential technologies**. Our ultimate goal is to support any technology for verifiable credentials by building an interface for the OpenDSU. As this interface is already in place, the next step is building adapters.

Identifying the entities in the network is important, and this is why the project opted to act as a root of trust for pharma companies for issuing verified credentials. This was the starting point since identification is a fundamental issue in every project.

### 4.2.4 Transition from Innovation to Industry & Pharma Specificity

**Q7: What are the challenges in transitioning from innovation to operation?**

**A7:** The first **challenge** to account for is the **funding**, as the transformation needs an investment. It is vital to showcase the value that a new technology carries toward the business needs. Besides the hype, the logical points to present are the revenue raise and the cost reduction for business. Corporate companies are interested in trying and implementing new technological trends because innovation is a key driver. But this relates to the point of investing small amounts and resources in having a proof of concept and figuring out if the technology is beneficial on a large scale. The next challenge is to build a **business case out of the proof of concept**, as companies have grasped how the technology works and its benefits. This is the most crucial and difficult point in the transition process, as the results and value coming from the investment are unclear and undefined. In other words, the return of investment and the business value should be clearly defined from the start. This is a weak point for blockchain, as there are no measured key performance indicators that can measure the cost-saving impact and many points remain unclear. Blockchain is a new technology that can be applied in many industries. We have promises and hope with all new technologies, but proving these points is challenging.

On top of that, there are assumptions in the evaluation process. For instance, we think blockchain will work as expected. But, as the technology is novel, there are **no reliable measurements** to evaluate the impact. The contrast is profound databases, and web fronts used to create applications, which have been widely used for years. In a blockchain, it is unclear **how the technology will be shaped** in the next few years. For instance, a question can be in the existence of Ethereum in five years' time or if it continues to be one of the leading blockchains. Its current state appears to be having issues with scaling as gas fees continue to skyrocket. This is because the network has become congested given the current hype of NFT's [non-fungible tokens]. Other competitors (e.g., Solana, Avalanche) are developing and releasing novel technologies and code that can address concerns related to the speed of transactions, scalability and whether the consensus mechanism used is eco-friendly (as most sceptics always focus on this topic). Just as previous pioneering internet companies

such as AltaVista and Yahoo took the first step, others such as Google and Facebook were able to dominate the market share.

Internet companies with initial success have missed some opportunities, and they disappeared. There are unknown issues in blockchain, like stability, scalability, reliability, and security. These issues make it difficult to convince business people to switch to blockchain in operation.

It takes a lot of time for small incremental steps **to convince communities** of new technology. For example, PharmaLedger took nine months to install a blockchain node in a productive environment. The reason for taking this time is that all quality and security policies should be upheld in the new application. The blockchain node operates differently from web servers, so education material and explanations should also be communicated with companies. After that, the next step is to align with other pharma companies and assess their state. Once the alignment is made, nodes are deployed, the testing phase comes to monitor the nodes' behaviour and the emerging problems from the operation. This is only on the technology level without diving into the business level.

On the business level, companies are willing to invest considerable funds to adopt blockchain technology internally. However, they have to be convinced about the **value and impact of the adoption**. Examples can be found from other technologies that are adopted. It is normal to build a platform to showcase the technology. Once the platform is deployed, new applications can be built on top of it. That was the case with AI or data translation services. However, this is not possible for blockchain, as there is a need to build an ecosystem with a different dimension compared with the other technologies. The transfer to a blockchain is much harder, as there is little value in adopting by a single company. The value is greater once an ecosystem is established with multiple stakeholders that utilise blockchain technology. That is why it is vital to convince multiple parties to join such an ecosystem.

It's important to clarify for the transition of research to adoption is the impact of the suggested solution. If there is only an improvement of 5% to 10%, there is little to no appetite to take the risk of implementing a novel technology. It might be counter-efficient to use new technologies for a feeble improvement due to the costs and risks involved in developing the application.

Another point that makes the adoption of blockchain difficult is the **lack of experience**. For instance, the discussions taking place in PharmaLedger to determine the appropriate governance indicate this. However, there are limited examples that have applied specific governance models. Moreover, it gets more complex as the project needs to define the requirements of the governance model. There are cases with similarities in the literature, like building a country's constitution, but it is mandatory to guarantee the balance in the power allocation. This is important for decentralised organisations to have a balanced power allocation and still make decisions.

**Q8: You've mentioned governance models. Are there particular governance setups in the pharma industry? Are those setups aligned with the blockchain logic on decentralisation?**

**A8:** Pharma companies have strict hierarchical governance of the organisation. This is similar to having third parties, middlemen, and intermediaries. Blockchain is trying to prevent this and strives for decentralising operations. There should not be a vendor lock-in dependency but rather aiming for independence. The challenge is convincing partners to **participate in funding, development, and decision-making** actively.

There are some traditional organisation structures where an association is built upon a membership fee, and this association establishes a **governance board** to make decisions. That may be the starting point, as the discussions in PharmaLedger revolves around this idea. But this should be only the initial step, as the association should evolve to a more decentralised structure and strive to become a decentralised autonomous organisation or so-called **DAO**. DAO's are the opposite extreme of the centralised entities: companies have to decide on their role in this future ecosystem as adoption drivers or be left on the side-lines. In my opinion, the right decision lies in striving to be leaders and pioneers in adopting blockchain technology solutions.

There are difficulties in the transition of pharma companies compared to software companies. The ultimate objective in the pharma industry is to create new medicines that can help patients. The correlation of results with the technology adoption is difficult, as the business will experience the change in 5 to 10 years for drug development. So, there is a need to come up with different solutions, as the **impact is in the long term**.

**Q9: Are there any recommendations or key messages that you would like to direct to any teams struggling for transition in the healthcare or pharma industry?**

**A9:** It is important to consider that traditional companies and industries are not like IT companies. The discussion is always on the agile methodology and the need to take risks. But the quote "**Crawl, Walk, Run**" always comes to my mind. Everyone starts their journey by crawling. Once they are comfortable with it, walking is the next phase. Once a project has set fundamentals while "crawling" and "walking", the "running" phase hits the ground for deploying a market application.

For PharmaLedger to succeed, all consortium members must work as one and **collaborate** in a way that allows blockchain technology to demonstrate value to patients ultimately. Given the number of stakeholders within the ecosystem, it can be hard to align internally on matters; however, the vision and power of building a digital trust ecosystem for the pharmaceutical industry and healthcare sector are truly pioneering. Building networks, platforms, and applications take time, and **refinement** must be in incremental steps critical for use case success. One aspect to focus on is decentralisation, and governance structures are being constructed to allow for an element of this. A positive outcome so far is the deployment of six blockchain nodes on a decentralised network for the electronic product information use case.

To prove success and bring value to the business is much more difficult in blockchain projects. Starting up with initiatives that have not proven to work yet means allocating funds and resources. In other words, willingness to risk can be costly, yet there may not be a success as a final result.

# CONCLUDING REMARKS

Blockchain is a novel technology used in numerous sectors and use cases and is especially **promising in healthcare** and COVID-19 pandemic management. Throughout this report, blockchain is presented from different angles, from healthcare data exchange transparency and medical credentialing to aiding in pandemic management. As addressed in this report, inefficiencies within healthcare related to supply chain and inventory management could also be addressed using blockchain technology. The use of medical equipment by healthcare facilities could be monitored to streamline maintenance of equipment and identify deficiencies or surpluses of devices in different geographical regions using AI and routing patients to facilities that are best able to treat them. Using blockchains as a ledger for recording provenance, vaccines and other life-saving drugs could be monitored and tracked from their origin to their current locations, thus reducing the misplacement or mislabelling of medicines and the risk of counterfeit. Moreover, an open and transparent supply chain based on a blockchain could be applied to improve clarity on logistics time- and location-wise, bringing trust that the information has not been tampered with. This could play a supportive yet crucial role if an outbreak occurs, allowing the responsible organisations and bodies to re-arrange resources or come to contingency plans reducing the delays. The analysed and presented **use cases are many and diverse**, but all rely on blockchain to **decentralise procedures** and **establish trust** in a multiple stakeholder environment.

In medical research and healthcare, blockchain can drive the development of numerous use cases and **synergies with other technologies** further. For instance, a transition from an organisation applying machine learning to a consortium striving for **federated learning**. Blockchain mitigates federated learning's issues and helps achieve fairness, accountability of the processes, mitigating threats, and driving the collaboration between organisations, serving as a global model from locally trained models, allowing the exchange of models without transferring the dataset. Or for example, blockchain applied together with **AI** can help verify AI patterns, which is especially valuable for healthcare in analysing the possible trend in emergency medical services. Advanced artificial intelligence used with the blockchain could also be used to support the development of new drugs for various diseases, reveal and trace hidden variables that may cause an illness – either from genetic information or lifestyle choices – or even provide insights into the effectiveness of treatments or the combination of treatments. Combining blockchain with deep learning enables a world driven by big data that can then be used to address current and unforeseen shortcomings in healthcare: based on the traceability of the data or transactions available through blockchain, **machine learning** could predict the locations of outbreaks during a pandemic a priori, thus potentially leading to fewer infections if measures actions are taken and improving the real-time allocation of resources.

It is argued that blockchain technologies may not be suitable for the healthcare environment because of the prevalence of personal data and the immutability of data recorded in distributed ledgers. However, there is room for applying blockchain more flexibly when **combined with off-chain** solutions. To comply with GDPR, products can use blockchain on a layer above databases, so it is possible to monitor transactions on the data exchange and access information while all personal health data is stored off the blockchain. Hence, the blockchain is merely used to record "digital fingerprints" of personal data which remain off-chain. Ultimately, we witness a large number of use cases that would benefit from the blockchain where traditional database technologies suffer from certain drawbacks such as lack of knowledge on *provenance, transparency*, *traceability*, *decentralisation*, and more *advanced application of business logic* (such as through smart contracts) supporting efficiency and accuracy of data-related processes. Leveraging all blockchain benefits from traceability to transparency could encourage trust in unknown or untrusted environments, which is especially important in cases involving and focusing on patients and the use of their data.

In addition, if **data integrity and sharing** can be addressed to **alleviate requirements under data protection rules**, blockchain has the potential to operate as a decentralised and distributed knowledge base of anonymised medical data. By using blockchain and off-chain solutions as a data repository, researchers can use the open data as training models in many machine learning applications. Nevertheless, **compliance to the GDPR** and its recommendations and regulations should always be accounted for, starting from the design stage of blockchain systems and solutions development.

Blockchain involves much more than a technological infrastructure. New ways of **governing data relationships and networks** are possible through blockchain. As this report has partly shared, there are blockchain technologies already have been implemented for healthcare with the emergence of large, international consortia and many promising case studies. As a result, blockchain can serve as a conduit for economic development (Allen *et al*., 2020) and creates opportunities to enact social good (Hughes, 2017). **Patients can be empowered** to access and leverage their own data with greater outreach to underserved members of the community (Allen *et al*., 2020). Therefore, blockchain can be a crucial driver of digital transformation in healthcare, which is also regarded in academic publications like Jahankhani & Kendzierskyj (2019).

Furthermore, healthcare is moving towards a digital transformation and a health system known as **Healthcare 4.0**, similar to the earlier change in other industries such as manufacturing - Industry 4.0 (Herman *et al*. 2016), focusing on smart and connected healthcare. We can learn some design principles from this earlier transformation that will be crucial in a digitally transformed healthcare system. The following six principles were proposed in the work of Herman *et al*. (2016).

- **Interoperability**: enable people and machines to communicate through data standards and standardised infrastructure.
- **Virtualisation**: technologies for interoperability, faster internet connections, and connected devices enable the movement of parts of the physical processes in healthcare to a virtual environment.
- **Decentralisation**: linking real-time data and users together facilitates autonomous decision-making and reduces the necessity of centralised services.
- **Real-time capability**: a higher proportion of connected devices and people enable changes in real-time.
- **Service orientation**: a shift from products to services based on accumulating data could adapt faster to market changes.
- **Modularity**: a higher degree of module-based delivery and configuration enables faster adoption of changing needs.

By default, blockchain is a technology that is **in line with these six principles**, especially decentralisation, interoperability, and virtualisation. So, it is highly likely that the use of blockchain in the healthcare sector will continue as the digital transformation advances. As a result, new use cases will arise, and new blockchain solutions tailored for the regulatory area of healthcare will emerge.

Unfortunately, there is the risk that elected officials and regulatory agencies could fall behind with these technological innovations and create legislation or interpretations that could unintentionally hinder the progress of this innovation. For healthcare, the main breakthroughs of blockchain technologies lay not in the technology but the **improved access to health information** and blockchain technologies enable new opportunities for health record interoperability, health data interconnectivity, and controlled data sharing (Zhang *et al*., 2018). Hence, it demonstrates that blockchain technology can offer more patient-centred health technology approaches within a secure infrastructure.

In conclusion, we encourage the European Commission to **facilitate future legislation** enabling progress for health information technologies, including blockchain technologies and providing ethical protections for patients and their health information. This is a significant undertaking, and therefore legislators and regulators must understand the possible benefits, challenges, and value of blockchain technologies for healthcare. Oversight of decentralised blockchain technologies requires a fresh perspective and continual education of advances to determine **how to integrate this technology into the current and future regulatory frameworks**. Along these lines, we advocate for regular review of regulations and guidelines to reflect the latest developments and debates that arise from this rapidly evolving technology.

As a general note, we encourage standardisation bodies to consider the **meaning of blockchain in healthcare applications**, how the term is used and what technologies should be included here to support the use cases of the healthcare domain. Currently, the description of blockchain utilisation tends to vary from a broad spectrum of both decentralisation and transparency. Healthcare would benefit from the future development and adaptation of the technology if the community could coordinate on characterising the technology anchored in the real world and those projects already implemented in the area. This will lower the bar for new entities in healthcare to take the leap to innovate using the appropriate directions and application of this new technology.

# REFERENCES

Abadi, M., Burrows, M., Lampson, B. and Plotkin, G., (1993) 'A calculus for access control in distributed systems', in ACM Transactions on Programming Languages and Systems (TOPLAS), 15(4), pp.706-734.

Abbas, Q. E., & Sung-Bong, J. (2019, February). A survey of blockchain and its applications. In 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) (pp. 001-003). IEEE.

Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2021). NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Software: Practice and Experience.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In 2017 IEEE technology & engineering management conference (TEMSCON) (pp. 137-141). IEEE.

Al-Issa, Y., Ottom, M. A., and Tamrawi, A. (2019) 'eHealth Cloud Security Challenges: A Survey', in Journal of Healthcare Engineering, vol. 2019, Article ID 7516035.

Alabdulkarim, Y., Alameer, A., Almukaynizi, M., & Almaslukh, A. (2021). SPIN: A Blockchain-Based Framework for Sharing COVID-19 Pandemic Information across Nations. Applied Sciences, 11(18), 8767.

Allard, C. T. and Krasowski, M. D. (2021) 'Data on the activation and utilisation of an electronic health record patient portal in an adult inpatient population at an academic medical center', Data in Brief, 35, p. 106806.

Allen, M. et al. (2020) Blockchain ethical design framework for healthcare. Washington, DC: Government Blockchain Association. Source. (Accessed: 29 October 2021).

Alles, M. and Gray, G. L. (2020). "The first mile problem": Deriving an endogenous demand for auditing in blockchain-based business processes, International Journal of Accounting Information Systems, 38, p. 100465

Alsahli, M. A., Alsanad, A., Hassan, M. M., & Gumaei, A. (2021). Privacy Preservation of User Identity in Contact Tracing for COVID-19-Like Pandemics Using Edge Computing. IEEE Access, 9, 125065-125079.

Amin, M. R., Zuhairi, M. F., & Saadat, M. N. (2021, January). Transparent Data Dealing: Hyperledger Fabric Based Biomedical Engineering Supply Chain. In 2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM) (pp. 1-5). IEEE.

Anderson, D., Gardner, G., Ramsbotham, J. and Tones, M., 2009. E-portfolios: developing nurse practitioner competence and capability. Australian Journal of Advanced Nursing, The, 26(4), pp.70-76.

Anderson, G. F., & Hussey, P. S. (2000). Population Aging: A Comparison Among Industrialized Countries: Populations around the world are growing older, but the trends are not cause for despair. Health affairs, 19(3), 191-203.

Ashkar, G. L., de Jesus, J., Vinnakota, N., Helms, N., Jack, W., Chien, W., & Taylor, B. (2021). Evaluation of decentralized verifiable credentials to authenticate authorized trading partners and verify drug provenance. Blockchain in Healthcare Today.

Axuall, Inc. and MetroHealth Announce Collaboration to Improve and Streamline Practitioner Credentialing. PR Newswire.2020. Source. (Accessed 01-12-2021).

Bayle, A., Koscina, M., Manset, D., & Perez-Kempner, O. (2018, December). When blockchain meets the right to be forgotten: technology versus law in the healthcare industry. In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp. 788-792). IEEE.

Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of blockchain within healthcare. Blockchain in healthcare today.

Bhatia, S., & Wright de Hernandez, A. D. (2019). Blockchain is already here. What does that mean for records management and archives? Journal of Archival Organization, 16(1), 75-84.

Bongaarts, J. (2015, January). Global fertility and population trends. In Seminars in reproductive medicine (Vol. 33, No. 01, pp. 005-010). Thieme Medical Publishers.

Braithwaite, J., Churruca, K., Ellis, L.A., Long, J., Clay-Williams, R., Damen, N., Herkes, J., Pomare, C. and Ludlow, K., (2017). Complexity science in healthcare. Sydney: Australian Institute of Health Innovation, Macquarie University 2017. Complexity science in healthcare. Sydney: Australian Institute of Health Innovation, Macquarie University.

Brall, C., Schröder-Bäck, P. and Maeckelberghe, E. (2019). 'Ethical aspects of digital health from a justice point of view', European Journal of Public Health, 29(Supplement_3), pp. 18–22.

Brett, J. (2020) U.S. Health Department Chief discloses functioning blockchain project to track Covid-19. Jersey City, NJ: Forbes. Source. (Accessed: 21 November 2021).

Calvaresi, D., Calbimonte, J. P., Dubovitskaya, A., Mattioli, V., Piguet, J. G., & Schumacher, M. (2019). The good, the bad, and the ethical implications of bridging blockchain and multi-agent systems. Information, 10(12), 363.

Capece, G., & Passiatore, D. (2021). Blockchain during COVID-19: The Technology to Help Society. Sustainability, 13(18), 10478.

Chadwick, D. W., Laborde, R., Oglaza, A., Venant, R., Wazan, S., & Nijjar, M. (2019). Improved identity management with verifiable credentials and FIDO. IEEE Communications Standards Magazine, 3(4), 14-20.

Charles, W. M. (2021a) 'Accelerating life sciences research with blockchain', in Namasudra, S. and Deka, C. G. (eds) Applications of blockchain in healthcare. Singapore: Springer, pp. 221–252.

Charles, W. M. (2021b) 'Blockchain innovations in healthcare', PECB Insights, (33), pp. 6–11.

Charles, W., & Magtanong, R. (2022). Ethical Benefits and Drawbacks of Digitally Informed Consent. In Applied Ethics in a Digital World (pp. 101-123). IGI Global

Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. ecancermedicalscience, 11, p. 709

Clavel, N., Paquette, J., Dumez, V., Del Grande, C., Ghadiri, D. P., Pomey, M. P., & Normandin, L. (2021). Patient engagement in care: A scoping review of recently validated tools assessing patients' and healthcare professionals' preferences and experience. Health Expectations.

Comaniciu, D., Engel, K., Georgescu, B., & Mansi, T. (2016). Shaping the future through innovations: from medical imaging to precision medicine. Medical image analysis, 33, 19-26.

Edenberg, E., & Jones, M. L. (2019). Analyzing the legal roots and moral core of digital consent. New Media & Society, 21(8), 1804-1823

El-Toukhy, S., Méndez, A., Collins, S., & Pérez-Stable, E. J. (2020). Barriers to patient portal access and use: Evidence from the health information national trends survey. The Journal of the American Board of Family Medicine, 33(6), 953-968.

European Commission. (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions. EUR-Lex - 52020DC0066 - EN - EUR-Lex. Brussels. Source. (Accessed: 29 October 2021).

European Economic and Social Committee (2019) Opinion of the European Economic and Social Committee on blockchain and the EU single market: What next? INT/885 – EESC-2019-02261-00-00-AC-TRA. 547TH EESC Plenary Session 2019. Source. (Accessed: 29 October 2021).

European Medicines Agency (2020) Call to pool research resources into large multi-centre, multi-arm clinical trials to generate sound evidence on COVID-19 treatments. Amsterdam. Source. (Accessed: 21 November 2021).

European Parliament (2020) European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation, as amended 2020. EUR-Lex - 52018IP0373 - EN - EUR-Lex (2020/C 011/03). Source. (Accessed: 29 October 2021).

Evangelatos, N., Özdemir, V. and Brand, A. (2020) 'Blockchain for digital health: Prospects and challenges', Omics, 24(5), pp. 237–240.

Fitzsimons, J. K., Mantri, A., Pisarczyk, R., Rainforth, T., & Zhao, Z. (2020, August). A note on blind contact tracing at scale with applications to the COVID-19 pandemic. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-6).

Garg, C., Bansal, A., & Padappayil, R. P. (2020). COVID-19: prolonged social distancing implementation strategy using blockchain-based movement passes. Journal of Medical Systems, 44(9), 1-3.

Gopal, G., Suter-Crazzolara, C., Toldo, L., & Eberhardt, W. (2019). Digital transformation in healthcare–architectures of present and future information technologies. Clinical Chemistry and Laboratory Medicine (CCLM), 57(3), 328-335

Hamming, R. W. (1950). Error detecting and error correcting codes. The Bell system technical journal, 29(2), 147-160Hamming, R.W. (1950) 'Error detecting and error correcting codes', in The Bell System Technical Journal, vol. 29, no. 2, pp. 147-160.

Haque, A. K. M., Naqvi, B., Islam, A. K. M., & Hyrynsalmi, S. (2021). Towards a GDPR-compliant blockchain-based COVID vaccination passport. Applied Sciences, 11(13), 6132.

Harris, R. E. (2019). Epidemiology of chronic disease: global perspectives. Jones & Bartlett LearningHarris, R.E., 2019. Epidemiology of chronic disease: global perspectives. Jones & Bartlett Learning.

Hashed Health. (2021, 01 December). A Digital Exchange for Professional Credentials Data. Hashed Health. 2020. Source.

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, 512-529.

Hasselgren, A., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2021). Medical Students' Perceptions of a Blockchain-Based Decentralized Work History and Credentials Portfolio: Qualitative Feasibility Study. JMIR Formative Research, 5(10), e33113

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics, 134, 104040.

Hasselgren, A., Rensaa, J. A. H., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2021). Blockchain for increased trust in virtual health care: proof-of-concept study. Journal of Medical Internet Research, 23(7), e28496.

Hasselgren, A., Wan, P. K., Horn, M., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2020). GDPR Compliance for Blockchain Applications in Healthcare. arXiv preprint arXiv:2009.12913. Source.

Health Information and Management Systems Society (2020) Interoperability in healthcare. Chicago: HIMSS. Source. (Accessed: 23 November 2021).

Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. Law, Innovation and Technology, 12(1), 156-174.

Hermann, M., Pentek, T., & Otto, B. (2016, January). Design principles for industrie 4.0 scenarios. In 2016 49th Hawaii international conference on system sciences (HICSS) (pp. 3928-3937). IEEE.

Herzberg, A., Mass, Y., Mihaeli, J., Naor, D., and Ravid, Y. (2000) 'Access control meets public key infrastructure, or: assigning roles to strangers', in Proceeding 2000 IEEE Symposium on Security and Privacy, S&P 2000, pp. 2-14.

Hirano, T., Motohashi, T., Okumura, K., Takajo, K., Kuroki, T., Ichikawa, D., ... & Ueno, T. (2020). Data validation and verification using Blockchain in a clinical trial for breast Cancer: regulatory sandbox. Journal of Medical Internet Research, 22(6), e18938.

Hughes, K. (2017). Blockchain, the greater good, and human and civil rights. Metaphilosophy, 48(5), 654-665.

Illingworth, P., & Chelvanayagam, S. (2017). The benefits of interprofessional education 10 years on. British Journal of Nursing, 26(14), 813-818.

Jahankhani, H., & Kendzierskyj, S. (2019). Digital transformation of healthcare. In Blockchain and Clinical Trial (pp. 31-52). Springer, Cham.

Joshi, P., & Gokhale, P. (2021). Electronic Health Record Using Blockchain and Off Chain storage: A systematic review. Information Technology in Industry, 9(1), 247-253.

Kamel Boulos, M. N., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. International journal of health geographics, 17(1), 1-10.

Katz, J. (2010). Digital signatures. Springer Science & Business Media.

Keys, Y., Silverman, S. R., & Evans, J. (2017). Identification of tools and techniques to enhance interdisciplinary collaboration during design and construction projects. HERD: Health Environments Research & Design Journal, 10(5), 28-38.

Khatter, K. (2021). Non-functional requirements for blockchain enabled medical supply chain. International Journal of System Assurance Engineering and Management, 1-13.

Khurshid, A. (2020). Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. JMIR medical informatics, 8(9), e20477.

Kritikos, M. (2020) Ten technologies to fight coronavirus. PE 641.543. Brussels: European Parliamentary Research Service.

Kumar, A. (2020). Improvement of public distribution system efficiency applying blockchain technology during pandemic outbreak (COVID-19). Journal of Humanitarian Logistics and Supply Chain Management.

Kumar, R., & Sharma, R. (2021). Leveraging blockchain for ensuring trust in IoT: A survey. Journal of King Saud University-Computer and Information Sciences.

Kumar, R., Khan, A. A., Kumar, J., Zakria, A., Golilarz, N. A., Zhang, S., ... & Wang, W. (2021). Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging. IEEE Sensors Journal.

Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine Generals Problem. In Concurrency: The Works of Leslie Lamport (pp. 203-226).

LaPointe, C. and Fishbane, L. (2019) The blockchain ethical design framework. Washington, DC: Georgetown University. Source. (Accessed: 26 September 2021).

Lemmon, A. (2021, May). Re-shaping the future of identity through user-owned verifiable credentials. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-2). IEEELemmon, A., 2021, May. Re-shaping the future of identity through user-owned verifiable credentials. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-2). IEEE.

Leon-Sanz, P. (2019). Key points for an ethical evaluation of healthcare big data. Processes, 7(8), 493Leon-Sanz, P. (2019) 'Key points for an ethical evaluation of healthcare big data', Processes, 7(8), p. 493.

L'Hutereau, A., Burihabwa, D., Felber, P., Mercier, H., & Schiavoni, V. (2019, October). Blockchain-Based Metadata Protection for Archival Systems. In 2019 38th Symposium on Reliable Distributed Systems (SRDS) (pp. 315-3158). IEEE

Lilani, S., Malani, D., Modi, J., & Soni, F. (2020). Securing the Software Development Life Cycle (SDLC) with a Blockchain Oriented Development Approach. Think India Journal, 22(41), 221-226.

Lin, H. Y., & Tzeng, W. G. (2010). A secure decentralized erasure code for distributed networked storage. IEEE transactions on Parallel and Distributed Systems, 21(11), 1586-1594

Lo, S. K., Liu, Y., Lu, Q., Wang, C., Xu, X., Paik, H. Y., & Zhu, L. (2021). Blockchain-based Trustworthy Federated Learning Architecture. arXiv preprint arXiv:2108.06912. Source.

Lopez, P. G., Montresor, A., & Datta, A. (2019, July). Please, do not decentralize the Internet with (permissionless) blockchains! In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS) (pp. 1901-1911). IEEELopez, P. G., Montresor, A. and Datta, A. (2019) 'Please, do not decentralize the Internet with (permissionless) blockchains!' Universitat Rovira i Virgili, Tarragona, Spain. Source. Source.

Lv, W., Wu, S., Jiang, C., Cui, Y., Qiu, X., & Zhang, Y. (2020). Towards large-scale and privacy-preserving contact tracing in COVID-19 pandemic: A blockchain perspective. IEEE Transactions on Network Science and Engineering.

Marbouh, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., ... & Ellahham, S. (2020). Blockchain for COVID-19: review, opportunities, and a trusted tracking system. Arabian Journal for Science and Engineering, 1-17.

Marotta, G., Fornaia, A., Moschitta, A., Pappalardo, G., & Tramontana, E. (2021, January). NausiChain: a Mobile Decentralized App Ensuring Service Continuity to University Life in Covid-19 Emergency Times. In 2021 The 4th International Conference on Software Engineering and Information Management (pp. 74-81).

Massaro, M. (2021). Digital transformation in the healthcare sector through blockchain technology. Insights from academic research and business developments. Technovation, 102386.

Maurer, U. (1996, September). Modelling a public-key infrastructure. In European Symposium on Research in Computer Security (pp. 325-350). Springer, Berlin, Heidelberg.

McQuinn, A. and Castro, D. (2019) A policymaker's guide to blockchain. Washington, DC: Information Technology and Innovation Foundation. Source. (Accessed: 29 October 2021).

Metcalf, D. S., Bass, J., Hooper, M., Cahana, A., & Dhillon, V. (2019). Blockchain in healthcare: Innovations that empower patients, connect professionals and improve care. CRC Press, Taylor & Francis Group.

MiPasa (2021) Analytics reDeFined. San Francisco. Available at: https://app.mipasa.com/ (Accessed: 21 November 2021).

Mondschein, C. F., & Monda, C. (2019). The EU's General Data Protection Regulation (GDPR) in a research context. In Kubben, P., Dumontier, M., & Dekker, A. (eds) Fundamentals of clinical data science. Cham: Springer, pp. 55-71

Monteiro, A. (2019) First GDPR fine in Portugal issued against hospital for three violations. Portsmouth, NH: International Association of Privacy Professionals. Source. (Accessed: 29 October 2021).

Morgan, M. W., Zamora, N., & Hindmarsh, M. F. (2007). An inconvenient truth: a sustainable healthcare system requires chronic disease prevention and management transformation. Healthcare Papers, 7(4), 6.

Nawale, S. D., & Konapure, R. R. (2021, June). Blockchain & IoT based Drugs Traceability for Pharma Industry. In 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-4). IEEE.

Nehme, M., Kaiser, L., Gillet, P., Thevoz, P., Stringhini, S., & Guessous, I. (2021). Digital COVID Credentials: An Implementation Process. Frontiers in Digital Health, 3, 70.

Nelson, R., & Staggers, N. (2016). Health Informatics-E-Book: An Interprofessional Approach. Elsevier Health Sciences.

Ng, W. Y., Tan, T. E., Movva, P. V., Fang, A. H. S., Yeo, K. K., Ho, D., ... & Ting, D. S. W. (2021). Blockchain applications in health care for COVID-19 and beyond: a systematic review. The Lancet Digital Health, 3(12), e819-e829.

Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2021). Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. Ieee Access, 9, 95730-95753.

Odoom, J., Soglo, R. S., Danso, S. A., & Xiaofang, H. (2019, December). A Privacy-preserving Covid-19 Updatable Test Result and Vaccination Provenance based on Blockchain and Smart contract. In 2019 International Conference on Mechatronics, Remote Sensing, Information Systems and Industrial Information Technologies (ICMRSISIIT) (Vol. 1, pp. 1-6). IEEE.

Omar, I. A., Jayaraman, R., Salah, K., Yaqoob, I., & Ellahham, S. (2021). Applications of blockchain technology in clinical trials: Review and open challenges. Arabian Journal for Science and Engineering, 46(4), 3001-3015.

Osmanlliu, E., Rafie, E., Bédard, S., Paquette, J., Gore, G., & Pomey, M. P. (2021). Considerations for the Design and Implementation of COVID-19 Contact Tracing Apps: Scoping Review. JMIR mHealth and uHealth, 9(6), e27102.

Ouyang, L., Yuan, Y., Cao, Y., & Wang, F. Y. (2021). A novel framework of collaborative early warning for COVID-19 based on blockchain and smart contracts. Information Sciences, 570, 124-143. Source.

Peng, S., Bai, L., Xiong, L., Qu, Q., Xie, X., & Wang, S. (2021, March). GeoAI-based Epidemic Control with Geo-Social Data Sharing on Blockchain. In 2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM) (pp. 1-6). IEEE.

Plank, J. S., & Thomason, M. G. (2003). On the practical use of ldpc erasure codes for distributed storage applications. Technical Report CS-03–510.

Platt, M., Hasselgren, A., Román-Belmonte, J. M., De Oliveira, M. T., De la Corte-Rodríguez, H., Olabarriaga, S. D., ... & Mackey, T. K. (2021). Test, Trace, and Put on the Blockchain?: A Viewpoint Evaluating the Use of Decentralized Systems for Algorithmic Contact Tracing to Combat a Global Pandemic. JMIR Public Health and Surveillance, 7(4), e26460.

Porsdam Mann, S., Savulescu, J., Ravaud, P., & Benchoufi, M. (2021). Blockchain, consent and prosent for medical research. Journal of medical ethics, 47(4), 244-250.

Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. Health and technology, 7(4), 441-451.

Rakib, G. A., Islam, M. S., Rahman, M. A., Syed, A. M., Hossain, M. S., Alrajeh, N. A., & El Saddik, A. (2021, June). DeepHealth: A Secure Framework to Manage Health Certificates Through Medical IoT, Blockchain and Deep Learning. In 2021 IEEE International Symposium on Medical Measurements and Applications (MeMeA) (pp. 1-6). IEEE.

Quito, A. (2021). More than 450 airlines can now use IBM's blockchain-based vaccine passport. New York: Quartz. Source. (Accessed: 21 November 2021).

Sadri, S., Shahzad, A., & Zhang, K. (2021, February). Blockchain traceability in healthcare: Blood donation supply chain. In 2021 23rd International Conference on Advanced Communication Technology (ICACT) (pp. 119-126). IEEE.

SERIES, B.P., 2020. Opportunities and Challenges of Blockchain Technologies in Health Care.

Sharma, T. K. (2019) Permissioned and permissionless blockchains: A comprehensive guide. Walnut, CA: Blockchain Council. Source. (Accessed: 29 October 2021).

Shuaib, M., Alam, S., Alam, M. S., & Nasir, M. S. (2021). Compliance with HIPAA and GDPR in blockchain-based electronic health record. Materials Today: Proceedings.

SICPA (2021) Tamper-proofing certificates. Lausanne, Switzerland: SICPA Holding SA. Source. (Accessed: 22 November 2021).

Son, H., Nahm, E. S., Zhu, S., Galik, E., Seidl, K. L., Van de Castle, B., & Russomanno, V. (2021). Testing a model of patient portal use in adult patients. Journal of Nursing Scholarship, 53(2), 143-153.

Steinwandter, V. and Herwig, C. (2019) 'Provable Data Integrity in the Pharmaceutical Industry Based on Version Control Systems and the Blockchain', PDA Journal of Pharmaceutical Science and Technology, 73(4), pp. 373–390.

Stolfo, S. J., Hershkop, S., Bui, L. H., Ferster, R., & Wang, K. (2005, May). Anomaly detection in computer security and an application to file system accesses. In International Symposium on Methodologies for Intelligent Systems (pp. 14-28). Springer, Berlin, Heidelberg.

Tang, Y., Xiong, J., Becerril-Arreola, R., & Iyer, L. (2019). Ethics of blockchain: a framework of technology, applications, impacts, and research directions. Information Technology & People.

Tobiano, G., Jerofke-Owen, T., & Marshall, A. P. (2021). Promoting patient engagement: A scoping review of actions that align with the interactive care model. Scandinavian Journal of Caring Sciences, 35(3), 722-741.

Tresp, V., Overhage, J. M., Bundschus, M., Rabizadeh, S., Fasching, P. A., & Yu, S. (2016). Going digital: a survey on digitalization and large-scale data analytics in healthcare. Proceedings of the IEEE, 104(11), 2180-2206V.

Uddin, M., Salah, K., Jayaraman, R., Pesic, S., & Ellahham, S. (2021). Blockchain for drug traceability: Architectures and open challenges. Health Informatics Journal, 27(2), 14604582211011228.

Umbrello, S., & Van de Poel, I. (2021). Mapping value sensitive design onto AI for social good principles. AI and Ethics, 1(3), 283-296. https://doi.org/10.1007/s43681-021-00038-3

Vaas, L. (2021) UPDATE: EU's Green Pass Vaccination ID private key leaked or forged. Woburn, MA: Threatpost. Source. (Accessed: 22 November 2021).

Vervoort, D., Guetter, C. R., & Peters, A. W. (2021). Blockchain, health disparities and global health. BMJ Innovations, 7(2).

Vezyridis, P., & Timmons, S. (2021). E-Infrastructures and the divergent assetization of public health data: Expectations, uncertainties, and asymmetries. Social Studies of Science, 0306312721989818

Watts, J., Yu, H., & Yuan, X. (2010, March). Case study: Using smart cards with pki to implement data access control for health information systems. In Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon) (pp. 163-167). IEEE

Wen, Z., Yu, K., Qi, X., Sato, T., Katsuyama, Y., Sato, T., ... & Hashimoto, J. (2021, March). Blockchain-Empowered Contact Tracing for COVID-19 Using Crypto-Spatiotemporal Information. In 2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM) (pp. 1-6). IEEE.

Williamson, L. M., & Devine, D. V. (2013). Challenges in the management of the blood supply. The Lancet, 381(9880), 1866-1875.

Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. Nature communications, 10(1), 1-8.

World Health Organization. (2021). Ethics and governance of artificial intelligence for health: WHO guidance.

Wu, H. T., & Tsai, C. W. (2018). Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing. IEEE Consumer Electronics Magazine, 7(4), 65-71.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. Report NISTIR 8202. Gaithersburg: National Institute of Standards and Technology.

Yu, K., Tan, L., Shang, X., Huang, J., Srivastava, G., & Chatterjee, P. (2020). Efficient and privacy-preserving medical research support platform against covid-19: A blockchain-based approach. IEEE consumer electronics magazine, 10(2), 111-120.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.

Zyskind, G., & Nathan, O., & Pentland, A. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.