BLOCKCHAIN™ IN HEALTHCARE TODAY

USE CASE

Ensuring Trust in Pharmaceutical Supply Chains by Data Protection by Design Approach to Blockchains

Halid Kayhan

KU Leuven Centre for IT & IP Law (CiTiP), Leuven, Belgium

Corresponding author: Halid Kayhan, Email: halid.kayhan@kuleuven.be

Keywords: blockchain, data protection by design, EU General Data Protection Regulation (GDPR), pharmaceutical supply chain, trust

Abstract

Pharmaceutical supply chains are complex structures that include various participants. Furthermore, blockchains are viewed as a promising solution to increase effectiveness and overcome some of the main challenges in these supply chains—especially lack of trust. The European Union (EU) set strict rules in the domain of pharmaceutical supply chains in order to protect patient safety and public health. In addition, blockchains bring legal requirements. Among these requirements, personal data protection is of utmost importance. This is because, as has been argued for years, blockchains and the EU data protection regime are in conflict by their natures. However, it is also claimed that when rightly designed and combined with other technological solutions, blockchains potentially offer great opportunities to enhance data protection. Nevertheless, potential for blockchains in the pharmaceutical supply chain is not yet been realized as most use cases are in the proof of concept or pilot stage.

This article examines the debates surrounding blockchains and data protection. The goal is to draw constructive conclusions on whether blockchain solutions can be designed in data protection-enhancing ways and whether this might help realize the potential for blockchain in pharmaceutical supply chains—particularly by creating trust. For this purpose, the example of an ongoing EU-funded innovative research project called PharmaLedger as a case study to concretize its theoretical examinations is examined. This project is chosen because it gathers a wide variety of stakeholders representing different interests and aims to create a digital trust ecosystem in health care by providing a widely trusted platform that supports the design and adoption of blockchain-enabled healthcare solutions while accelerating the delivery of innovation that benefits the entire ecosystem from manufacturers to patients.

Received: April 29, 2022; Revised: July 20, 2022; Accepted: August 7, 2022; Published: September 5, 2022

Blockchain is a class of technology used for various purposes. However, the increasing number of use cases indicates that blockchain still has much to offer. On the other hand, the considerable number of projects at the proof of concept or pilot stage suggests that launching a successful blockchain use case is not always straightforward.[1]

It should be made clear at the start that although they are used interchangeably by many writers, blockchain is one type of distributed ledger technology. Blockchain offers a sequential, verifiable, and incremental way to record data.[2] Basically, this particular type of technology acts as a decentralized append-only database that is maintained by a consensus algorithm and kept across a peer-to-peer network of numerous nodes (computers).[3] While all nodes are located outside of or connected with one central node in centralized software systems, the nodes in decentralized systems do not require a central element of coordination or control while forming a network of connected nodes. In addition to immutability, prominent features of a blockchain network include transparency, auditability, and robustness.[2]

While traditional database technologies suffer from drawbacks such as the lack of information on provenance, transparency, and traceability among many others, blockchains, contrarily, benefit from traceability

and transparency, as well as decentralization and more advanced application of business logic—as carried out by smart contracts. All this increases efficiency and accuracy of data-related processes. These advantages offered by blockchains encourage trust in health care in various use cases.[4] Among these, pharmaceutical supply chains require particular attention due to their critical role in the protection of patient safety and public health.

The healthcare sector, and especially pharmaceutical supply chains, is highly regulated in the EU. Thus, the success, or sometimes even launch, of any blockchain use case in this area strongly depends on its compliance with the applicable legal frameworks, particularly on data protection and privacy.

To concretize this analysis, this article takes the example of the ongoing PharmaLedger project, which aims to provide a widely trusted platform that supports the design and adoption of blockchain-enabled healthcare solutions in different domains, including the pharmaceuticals supply chain, while accelerating delivery of innovation that benefits the entire ecosystem from manufacturers to patients.[5] By doing so, the author explores whether the claims that blockchain-enabled supply chain management practices could solve the main challenges in pharmaceutical supply chains,[1] particularly the lack of trust,[4] while also ensuring data protection compliance by the appropriate design of the technology.

This paper will first briefly explain the potential of the blockchain in the pharmaceutical supply chains and, then, give an overview of the legal framework applicable to these supply chains in the EU. Considering the long-lasting debates around the conflicts between the EU data protection regime and blockchains, this issue will be examined in detail in the context of pharmaceutical supply chains in a separate section. Finally, as a case study, the PharmaLedger project will be assessed in order to see whether this project, funded under the EU's Horizon 2020 research and innovation programme,[5] manages to provide some solutions for compliance with the strict rules under the EU data protection regime.

Blockchain in Pharmaceutical Supply Chains

As one of the most complex supply chains in the world, the pharmaceutical supply chain is vulnerable to opacity.[6] Transparency in supply chains is challenging due to, but not limited to, the global nature of the industry, the size and scope of the companies, the number of different players involved, manual data processing, and the use of databases that are not interconnected, as well as complex data flow among players.[7]

In pharmaceutical supply chains, drugs change hands among multiple players, such as manufacturers, distributors, repackagers, wholesalers, and subcontractors before reaching the patient. This results in vulnerabilities to theft, introduction of fake medicines into legal chains, and non-compliance. In addition, these chains rely heavily on different forms of transportation and communication channels (e.g., airlines, airports, freight forwarders, trucking agencies, and third-party logistics), and this creates "dark matter gaps" in supply chain transparency.[8]

As noted in a recent report by the EUBlockchain Observatory and Forum, blockchain can have a significant impact on pharmaceutical supply chains where traceability and transparency are key elements. In these complex ecosystems, which include numerous parties, information sharing is asymmetrical, and the parties involved receive updates with a time lag. Moreover, due to the silos, duplication of tasks and information is common. Blockchain, at this point, can increase efficiency of the procedures.[4]

The European Commission, in its Pharmaceutical Strategy for Europe, published in 2020, supports implementation of strategic actions.[9] Although it does not explicitly discuss blockchain as a solution, blockchain technology has the potential to assist several actions and concerns, such as silos and transparency. Indeed, it is possible to see more self-evident use cases in the pharmaceutical sector. For instance, blockchain could be used for the purposes of finished goods traceability and anti-counterfeiting.[4] The World Health Organization, in a study dated 2017, estimates that 10% of medical products are falsified,[10] and this is seen as a growing threat by the sector. Considering this and the demand that occurs as a result, for use cases in the contexts of anti-counterfeiting,[4] as well as finished goods traceability to identify shortages—as the COVID-19 pandemic showed—blockchains could support safe and efficient processes.[11]

In addition, the same report by the EU Blockchain Observatory and Forum highlights that blockchain can address inefficiencies related to supply chain and inventory management within health care. This class of technology can be used as a ledger to record the provenances of pharmaceutical products, and thus, vaccines and other life-saving drugs can be monitored and tracked throughout their journey. This will result in reducing the misplacement or mislabeling of medicines and the risk of counterfeiting. A transparent blockchain-based supply chain can also serve to improve clarity on logistics time and location and create trust that the information has not been tampered with. In case of an outbreak such as COVID-19, this can offer an important opportunity for responsible entities to rearrange resources or produce contingency plans to avoid delays.[4] The potential benefits of blockchains in the management of pharmaceutical supply chains are listed in the literature as follows:

- decreasing or effacing frauds and errors,
- decreasing the number of delays due to paperwork,
- decreasing courier costs,
- more rapid determination of relevant issues,
- improved inventory management,
- creating greater trust for consumers and partners.

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

It must be added that this potential is not yet fulfilled and requires further resources, research, and maturation of real-life use cases, which are mostly at proof of concept or pilot stages, and new technological solutions.[1]

PharmaLedger, an innovative research project funded by the EU, is designed to create a digital trust ecosystem in health care. More specifically in the context of supply chains, it aims to improve patient safety and product traceability by laying the groundwork for the use of blockchain technology and serialization throughout the medicine supply chain. By gathering numerous actors with different interests, this project also has an objective of developing a scalable, sustainable, technology agnostic, blockchain-enabled platform that can be adopted by the whole healthcare ecosystem for various use cases. This begs the question of whether it could provide the necessary solutions to fulfill the above-mentioned potential of blockchains in pharmaceutical supply chains, but also more generally in health care.[5] Although there may be many different blockchain applications in the context of pharmaceutical supply chains, the PharmaLedger Project, with its several use cases in the pharmaceutical supply chains domain, could serve as a useful example for analysis based on concrete cases.

Overview of the Legal Framework in the EU

Pharmaceutical supply chains are subject to strict regulations in the EU. As a result, there is heavy oversight in order to protect the public from harmful drug effects. A comprehensive strategy covering all levels of the pharmaceutical value chain, from research and development through authorization, distribution, and patients' access to medicines is crucial to ensure a high level of public health protection, starting prior to bringing new pharmaceuticals to market.[12]

The key applicable regulatory instruments, inter alia, are:

- Directive 2001/83 on the Community code for medicinal products for human use,[13]
- Directive 2003/94 on the principles and guidelines of good manufacturing practice,[14]
- Directive 2011/62 on falsified medicines (Falsified Medicines Directive),[15]
- Council of Europe Convention on the counterfeiting of medical products (the MEDICRIME Convention),[16]
- Regulation 2016/161 on safety features on the packaging of medicinal products,[17]
- Regulation 2020/1056 on electronic freight transport information,[18] and
- Regulation 726/2004 on authorization procedures and establishing European Medicines Agency.[19] Available at URL: https://health.ec.europa.eu/system/files/2016-11/reg_2004_726_en_0.pdf

These regulations require taking various aspects into account, including, but not limited to, market authorization requirements, safety measures, and reporting falsifying medicines in pharmaceutical supply chains regardless of deploying blockchain-enabled solutions.

Furthermore, sustainable management of supply chains, environmental considerations, human rights issues related to supply chains, and due diligence in sustainable supply chains should all be addressed in pharmaceutical supply chains. One reason for this is the fact that participants' visibility in most traditional supply chain networks is limited to their direct relationships one level up and down, but transparency and integrity of those supply chains must be assured by adopting a common approach to sustainable supply chain management, which provides further insight into the whole journey of a pharmaceutical product. Ensuring regulatory compliance will not be sufficient for such a strategy to be successful. Long-term sustainability and respect for human rights will also be needed.[20]

In addition to these strict regulations applicable to pharmaceutical supply chains, privacy and data protection require particular attention because, according to many, blockchain and the principles and obligations of the EU General Data Protection Regulation (GDPR)[21] are viewed as contradictory with each other.[22] For this reason, this issue will be explained separately in the following section of this article.

Privacy and Data Protection

Despite being used interchangeably from time to time in different jurisdictions, privacy and data protection are two separate but interrelated concepts. The Charter of Fundamental Rights of the European Union (CFREU) has, indeed, regulated these two rights in two separate articles—Articles 7 and 8. While the former article defines the right to privacy as "the right for respect for his or her private and family life, home and communications." The latter refers to "the right to the protection of personal data concerning him or her." Article 8, in addition to defining a separate right, lays down the core principles for the effective implementation of this right in paragraphs 2 and 3. It states that the processing of personal data must be fair, for specific purposes, and based on either the individual's consent or a legal basis. Individuals must have the right to access and correct their personal data; and compliance with these principles must be monitored by an independent authority.[23] The two rights are closely related because they both aim to uphold similar values, such as individual autonomy and human dignity. For this reason, they provide individuals with a personal sphere to freely develop their personalities and opinions. Nevertheless, their formulations and scopes differ under the CFREU. While the right to privacy entails a general prohibition

on interference with one's private life unless some public interest criteria are met to justify such interference in certain circumstances, the right to personal data protection is considered an active right bringing a system of checks and balances in order to protect individuals whenever they are subject to data processing. This makes the right to personal data protection broader than the right to privacy because a demonstration of an infringement of privacy is not necessary for the personal data protection principles to apply.[24]

With recent technological and organizational developments processing more and more personal data, data protection has become a prominent concern worldwide, and this has resulted in numerous legislation worldwide. In this paradigm shift, the EU is seen to have a particular role since, with its strict rules, it is considered the standard-setter on how new technologies should be developed and used to process personal data.[12] The GDPR, adopted in May 2016 and entered into force on 25 May 2018 by replacing the Data Protection Directive (Directive 95/46/EC),[25] is the main instrument in the EU's data protection law. Different from the Directive, the GDPR does not need to be transposed into the national laws of each EU Member State, but its rules are directly applicable in every EU Member State. Furthermore, considering the GDPR being widely seen as a high-watermark of data protection laws worldwide (and becoming a template for more and more countries' own legislation), developing a GDPR-compliant blockchain solution will support achieving data protection and privacy compliance not only at the European level but also globally as well.[26]

Legal issues to tackle while deploying blockchain not only are related to healthcare applications but also have greater significance for these applications due to the health sector's critical nature, and data protection is one of the most pressing legal concerns. A considerable amount of the data circulating within health care is sensitive, which requires greater protection. Thus, the principles of medical confidentiality, in addition to privacy and data protection, are of high importance. Certain risks associated with patient visibility and monitoring may be brought by blockchain-based applications, as well as the creation of aggregated profiles of patients if multiple sources data are combined. Stigmatization and discrimination may be seriously suffered by patients in case of data breaches. For these reasons, privacy and data protection should be seen as the main legal and ethical issues to be addressed while designing, deploying, and maintaining a blockchain-based healthcare solution.[4]

It is alleged by many that blockchains (particularly public, permissionless blockchains) are incompatible with the GDPR by their very nature since the GDPR was designed for centralized methods of data collection, processing, and storage while blockchains decentralize these methods.[3] Years after the GDPR came into force, its compatibility with the public permissionless blockchains is still highly disputable, but addressing the same issue in the cases of private, permissioned blockchains is more straightforward.

Since the core of this article is how to use blockchain technology in a GDPR-compliant way for the purposes of pharmaceutical supply chains, the focus is on private, permissioned blockchains. This is because supply chains require known parties in order for the participants to ascertain the source and quality of their inventory.[27]

As the disputes around data protection and blockchains are not only related to supply chain use cases, explanations will be given with a broader approach in this section, and, when needed, elaboration will be provided in the context of supply chains. In other words, these explanations can mostly be applied to different types of blockchain use cases as well.

A Closer Look at the Blockchain-GDPR Relationship

Taking the above-mentioned tensions into account, any blockchain use case that might process personal data should only take place after in-depth considerations and assessments regarding data protection. This is, indeed, true for pharmaceutical supply chains as privacy and data protection aspects with regard to health care are seen as one of the greatest challenges to realizing the potential of blockchains in this domain.[1]

A study conducted for the members and staff of the European Parliament explains that there are numerous tensions between the GDPR and blockchains due to two main reasons as listed below:

1. The GDPR is founded on the assumption that in each data processing activity, there is always at least one natural or legal person ("data controller") who is responsible for compliance with the GDPR and who can be requested to fulfill the rights of the data subjects in case such a request comes from their side. However, in blockchains and particularly in public, permissionless blockchains, there is not a central actor in control, as this is sought to be achieved by those blockchains. As a consequence, it is difficult to allocate the responsibility and accountability.
2. While the GDPR was being written, it was also assumed that in case of necessity to comply with Articles 16 ("Right to Rectification") and 17 ("Right to Erasure") of the GDPR, data could be modified or deleted. However, blockchains purposefully make such modifications extremely difficult, with the objective of ensuring data integrity and providing greater trust in the network. Uncertainties in the EU data protection regime, such as how the "erasure" concept needs to be understood, make it even more difficult to comply with the law.[22]

Before diving into the domains where these factors cause further difficulties, it is worth stating that despite

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

the tensions, blockchains also propose opportunities to achieve certain objectives of the GDPR. First of all, besides decentralized handling of personal data, blockchains promise data sovereignty, which is a concept focusing on giving data subjects control over their data and the opportunity for them to share their personal data only with the parties they trust. As indicated in its Recital 7, the GDPR has set data sovereignty as one of its objectives by giving natural persons "control over their data." Article 20 GDPR on the right to data portability enshrines this objective of data sovereignty by allowing data subjects the ability to receive their personal data from the data controller and to give it to another data controller. This right is seen as a concept stipulated in the GDPR with the purpose of giving more control to data subjects over their personal data.[3] As noted by the Article 29 Working Party, which is replaced by the European Data Protection Board (EDPB), the "primary aim of the data portability is enhancing individuals' control over their personal data and making sure that they play an active part in the data ecosystem."[28]

Another important point noted in the literature is the lack of exact definitions of data portability and data sovereignty in the GDPR or elsewhere. This is highly important because there are currently no solutions giving individuals full control over their personal data. Some solutions provide more control compared to others.[3] According to many, blockchains can be designed in a way that only the user is able to access the public and private keys and freely decide when to share their personal data with external parties.[29] With blockchains, selective data sharing is possible through applications, which ensure privacy and decrease the risk of identity theft.[3] Hence, new forms of identity management could be facilitated by blockchain by enabling individuals to control not just their identifiers but also the data associated with them.[30] Although there are still questions about certain points, such as whether parties with access to once revealed data will be able to copy and extract that data and store it permanently,[3] many new technological proposals for blockchains are under development in order to empower individuals to own and control their personal data.[31] Such developments in technology may offer means to achieve certain objectives of the GDPR.[3]

It is crucial to stress that blockchains do not, in themselves, provide guarantees to protect personal data, and they must be developed and deployed in combination with additional mechanisms in order to achieve data sovereignty objectives. Despite its strong promises for data sovereignty, blockchains may also reveal all the data stored on them unless the necessary safeguards are put in place. Since blockchains are still an emergent class of technology, they should be designed and developed in a fashion to fulfill technical and legal requirements and also according to policy considerations and what is desirable for the public good. In other words, despite the conceptual tensions with the GDPR, blockchains might realize some of the objectives of the GDPR through rightly developed technological means, which might be different from the mechanisms envisaged by the GDPR.[3] For instance, the append-only feature, which is also referred to as immutability, of blockchains offers the trust that data stored on the ledger have not been tampered with or manipulated. Blockchains can also enable better accountability by allowing visibility and traceability over who accesses data, thanks to time-stamped logs on the ledger. Furthermore, since the datasets are replicated across several computers, there is no single point of failure, and this guarantees data integrity and security.[2]

After setting the high-level scene, it is worth exploring the domains where blockchains are seen in conflict with the GDPR, and how these can be addressed. However, for the sake of brevity, these explanations will be succinct.

Types of Personal Data Processed on Blockchains

While the GDPR, as per Article 2, applies to the processing activities of personal data, Recital 26 states that anonymous data are not subject to the GDPR. This requires assessing what is personal data, and whether personal data processed on blockchains are classified as anonymous. Article 4 GDPR defines "personal data" as any information relating to an identified or, either directly or indirectly, identifiable natural person. On the other hand, Article 29 Working Party notes that anonymization occurs only in the cases of "processing personal data in order to irreversibly prevent identification."[32]

There are two types of data stored on blockchains that can be classified as personal data in the sense of the GDPR: transactional data and public keys. When transactional data are stored on a blockchain in plain text, it is obvious that it will be subject to the GDPR. However, even if data are encrypted, it will still be possible to access that data with the right keys, and, thus, those data will not be irreversibly anonymized.[3] Under the EU data protection law, encryption is regarded as a pseudonymization technique because an individual can still be indirectly identified.[32] In case transactional data are subject to hashing algorithms, those data will still be qualified as personal data for GDPR purposes[3] as Article 29 Working Party considers hashing as a pseudonymization method, given that the data subject and the dataset are still linkable.[32]

Nevertheless, it is also possible to store transactional data off-chain and only link those data to the blockchain with a hash pointer. Thus, personal data will be stored in a modifiable and encrypted database instead of the blockchain itself. By doing so, the concerns caused by the special features of blockchains from a data protection perspective will be avoided with regard to data stored off-chain.[3]

On the other hand, each participant of a blockchain network also has a unique personal identifier shared on the blockchain, which consists series of random-looking alphanumeric characters called the public key. This is a key to the participant's account, and when combined with the private key, which is known only by the participant, data encrypted with these keys will be decrypted. Participants randomly create this pair of public–private keys in their digital wallets, which is an application on a smartphone, computer, or another similar device. When a public key is associated with a natural person, public keys constitute personal data. Although these public keys are long strings of random-looking alphanumeric characters, they are not anonymous data under the EU data protection regime.[12] This is because the Article 29 Working Party classifies encryption with a secret key as a pseudonymization technique because "the holder of the [private] key [which is only known to the data subject in order to relate off-chain data with the public key] can trivially re-identify each data subject through decryption of the dataset."[32] This absolute approach of the Article 29 Working Party means that encrypted public keys on the chains should be treated as pseudonymous data because it is possible to reveal the identity behind those public keys by using additional information, which is the corresponding private key. When a public key is linked to a natural person, it will be possible to identify all previous transactions carried out by that person.[12] Different from transactional data, it is not possible to move public keys off-chain since they constitute part of the metadata transactions and are required for their validation, and, thus, they are essential for the functioning of the blockchain technology. As a result, it is more difficult to find GDPR-compliant solutions for public keys, compared to transactional data, which can be stored off-chain.[3]

Responsible Parties to Ensure Compliance

Since blockchain technology is based on the idea of decentralization, it is difficult, particularly in public, permissionless blockchains, to allocate the responsibility and accountability that are crucial for data subjects to find parties to address in order to enforce their rights under the GDPR. However, in supply chains, parties need to know other involved parties in order to ascertain the source and quality of their inventory. This will be only possible by using private, permissioned blockchains.

As recognized by the EU Blockchain Observatory and Forum, public permissionless blockchains represent the greatest challenge in terms of GDPR compliance, while it is easier for private permissioned blockchains to comply with the GDPR.[33] The strongly highlighted challenge of determining the controller significantly diverges from the initial public blockchains. With the technology and related business models being developed, this challenge appears to be less relevant for the many new multi-layered ecosystems that deploy new types of permissioned and consortium blockchains. Arguably, permissioned blockchains have been developed exactly in response to the shortcomings of public, permissionless blockchains.[34] When blockchain applications are built for proof and value transfer on top of a blockchain platform, there will almost certainly be a set of governance rules that represent the terms agreed upon by the ecosystem's participants to regulate their relationship.[35] These blockchains are permissioned in the sense that, depending on the governance model, one or several entities determine which parties are going to have permission to write.[2]

In a private, permissioned blockchain, the participants should determine their rights and obligations and document those in a governance model. A robust governance model should address the issue of responsibility allocation with regard to personal data protection as well as other regulatory issues, the competencies of the participants, and the procedures to ensure that data subjects can enforce their rights. Indeed, the French Data Protection Authority (CNIL) highlights the importance of taking a common decision about the data controllers' responsibilities in cases where a group of entities decides to carry out processing operations on a blockchain for a common purpose. The CNIL recommends either creating a legal person to be the data controller or designating the participant who makes decisions for the group as the data controller, and further notes that if neither of these is the case, all participants are likely to be considered as joint controllers.[36]

Thus, it is of utmost importance not only to establish a robust governance model to allocate the responsibility of data controllership but also to limit network access by allowing only trusted members to have the ability to add data onto the chain. By doing so, in addition to identifying the parties to be accountable by the authorities and data subjects, the number of threat actors and their affordance or capacity to enact privacy violations will be reduced.[4] The adopted governance model for any permissioned blockchain network should require all participants to agree to abide by the GDPR-compliant terms as a condition of being granted permission. The governance model should carefully consider the international data transfers and identify the most suitable mechanism and safeguards for the potential transfers of personal data to controllers and processors based outside the EU and not covered by an adequacy decision of the European Commission.[12] As per the *Schrems II* Decision of the Court of Justice of the EU,[37] the European Data Protection Board's recommendations on measures that supplement transfer tools,[38] and Clause 14 of the new standard contractual

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

clauses (SCCs) approved by the EC in June 2021—which will have completely replaced the three sets of SCCs adopted under the previous Data Protection Directive 95/46 by 27 December 2022[39]—an appropriate approach would be to oblige the members of the governance model to carry out a transfer impact assessment, through which data exporter and importer assess the impact on data protection of an international data transfer,[40] prior to each data transfer to a third country not covered by an adequacy decision.

Although this analysis is based on data protection, it is important to note that for blockchain use cases in the context of pharmaceutical supply chains, the governance model is critical beyond data protection and privacy.[2] One of the most important functions of product traceability is to provide the opportunity to identify the parties who are responsible for adverse impacts on consumers' safety, human rights, and sustainability. Identifying responsible actors is key to conducting a thorough examination of business relationships and assigning responsibility to them for adverse impacts. The governance model implemented by the authorized stakeholders is the basis of the transparency of the whole ecosystem. Thus, explicit guidelines for network administration should be provided by the governance model. It would be necessary to have legally enforceable contracts in order to document the relationship between the participants and network operators. Key issues that could be addressed by the governance models are as follows:

- participants' rights as well as obligations,
- procedures to make decisions and implement them,
- details and limits of the centralized control to be maintained,
- procedures to grant access permissions to the blockchain,
- parties that will validate transactions,
- responsibilities regarding the maintenance of the blockchain, commitments to participate in the platform's operation at the service level, and remedies for possible network downtime,
- measures to safeguard the maintenance of the network security,
- due diligence and participant monitoring mechanisms,
- rules and procedures to maintain data confidentiality among the participants.[41]

Regarding data controllership, as blockchains can grant data subjects more control over their data, another important question arises on whether they can be seen as data controllers where they hash their own data to a blockchain.[3] However, whether this argumentation will be accepted by the authorities is unclear for the time being.[2]

Data Protection Principles

European data protection regime is based on a number of key data protection principles, which are either explicitly stipulated in the relevant legislation, such as the GDPR and the Council of Europe Convention 108, or established through the case-law of the European Court of Human Rights and the Court of Justice of the European Union.[12] The data protection principles stipulated by Article 5 GDPR are as follows:

- lawfulness, fairness, and transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation;
- integrity and confidentiality;
- accountability.

It is important to note that among these principles, two seem particularly problematic: purpose limitation, which requires personal data to be processed only for an initially specified purpose, and data minimization, which requires processing only a minimum amount of data and for as long as it is necessary to achieve the purposes of the processing.[2]

With regard to the purpose limitation principle, the discussions are around whether it is compatible to further process personal data added to blocks following the execution of a transaction for which personal data were added to the chain in the first place.[22] As per the objective of enabling trust and reliability in a blockchain network, consensus algorithms establish a procedure in which each new block is added to the chain by involving some data from the previous block in order to maintain the ledger integrity. This makes those algorithms a crucial component of blockchain networks. Thus, it is argued that processing the hashed data continuously with the purpose of validation can be seen in compliance with the principle of purpose limitation. Nevertheless, it is also noted that such an argumentation will not be valid if the data are stored in plain text in public blockchains since disclosing personal data publicly will allow its further use by unknown third parties for whichever purposes.[2]

Turning to data minimization, Article 5(1)(b) GDPR stipulates that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." This principle is in conflict with the nature of blockchains, which are append-only databases and expand continuously. This is because once data are added to the chain, it will permanently be a part of the chain and when each block is added to the chain, more data will have been accumulated in the chain. Furthermore, contrary to the data minimization principle, each full node

stores a copy of the entire blockchain, and when new data are added to the chain, in principle, it is not possible to amend or delete it. However, by storing transactional data off-chain, it will be possible to minimize and amend those data without touching the chain itself in compliance with the data minimization principle. Nevertheless, it is more problematic to comply with this principle with regard to the pseudonymous public keys since it is not possible to remove those retroactively from the chain.[3] Noteworthy is that the French Data Protection Authority CNIL considers that these public keys are essential to the blockchain's proper functioning, and it is not possible to further minimize them. Thus, their retention period, which is the lifetime of the blockchain, is in line with the GDPR.[36]

Data Subject Rights

The effective exercise of data subject rights is essential to ensure the protection of personal data, and this is why data controllers are required to facilitate the exercise of these rights. The following is the list of rights granted to data subjects by the GDPR:

- Right to information (Articles 13 and 14 GDPR)
- Right to access (Article 15 GDPR)
- Right to rectification (Article 16 GDPR)
- Right to erasure (Article 17 GDPR)
- Right to restriction of processing (Article 18 GDPR)
- Right to data portability (Article 20 GDPR)
- Right to object (Article 21 GDPR)
- Right not to be subject to automated individual decision-making (Article 22 GDPR)

Two of these rights require attention since they raise particular challenges in the context of blockchains: the right to rectification and the right to erasure.

As stipulated by Article 16 GDPR, data subjects have the right to rectification, and this includes the right to obtain rectification from the data controller of inaccurate personal data without undue delay and to have incomplete personal data completed. This right is a reflection of the principle of accuracy under Article 5(1)(d) GDPR. According to this principle, controllers are obliged to take every reasonable step to ensure that personal data are accurate and, where necessary, kept up to date.

The (near-)immutability feature is built into the blockchain protocols with the purpose of creating trust in the network, and this feature, in principle, prevents any altering of data. However, this brings hurdles to fulfilling rectification requests that may come from data subjects.[2] While it can be possible to effectively exercise this right in permissioned blockchains by way of re-hashing subsequent blocks, it is not straightforward to find a solution in the case of permissionless blockchains.[42] As an alternative solution to direct modification of data on an append-only network, adding new information showing that the previously added data are incorrect is also suggested. In such a case, the most recent version will rectify the previous data and show the current status of that particular data. However, it is unclear, from a legal perspective, whether this is sufficient to comply with Article 16 of GDPR since the previously added, out-of-date, or inaccurate data will still be on the chain. It is also worth noting that the lack of the exact definition of "accuracy" in the GDPR does not help to solve this issue.[2] A more straightforward solution is to keep transactional data off-chain, and, by doing so, it will be possible to fulfill the request of rectification from data subjects in compliance with the GDPR since those data stored off-chain can be amended without touching the chain itself. However, this does not facilitate GDPR compliance in relation to public keys.[3]

On the other hand, Article 17 GDPR grants data subjects the right to erasure (also referred to as the "right to be forgotten"), which allows obtaining the data controller "the erasure of personal data concerning him or her without undue delay." It is important to note that this is not an absolute right as certain exceptions have been included in Article 17(2) GDPR. The tensions between this right and blockchains have been highlighted by many since blockchains' persistent and distributed architecture may render a straightforward deletion of data upon a request by data subjects impossible.[3,43] While erasing data in a single computer is always technically possible, erasure from one node in a blockchain network does not result in erasure in all nodes. Furthermore, such erasure, in most cases, would invalidate the node and pose a risk to the integrity of the blockchain network, which is crucial to creating trust.[2] It is once again essential to make a distinction between transactional data and public keys. While storing transactional data off-chain will significantly facilitate compliance with the requirements under Article 17, it is not straightforward to comply with erasure requests in the case of public keys, and this requires further explanations.[3]

As noted previously, the right to erasure is not an absolute right. Article 17(2) GDPR, indeed, says that in cases where data subjects request the erasure of their data, the data controller must take "account of available technology and the cost of implementation" and take "reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of those personal data." Considering this provision and blockchains' technical limitations to erasure as well as the lack of the exact definition of "erasure" in the GDPR, the question of whether a solution other than the outright erasure of data can be used in compliance with the GDPR becomes highly important. Some data protection authorities in Europe have indicated that "erasure" does not have to be the

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

outright destruction of personal data.[2] The UK Information Commissioner's Office tolerates, to a certain extent, putting data "beyond use" if it is not possible to delete the data for technical reasons.[44] The German act for adapting the data protection rules in Germany, adopted in accordance with the GDPR and German law, also puts a derogation to Article 17 GDPR and mandates that data controllers are not obliged to erase personal data where erasure is impossible or requires a disproportionate effort because of the specific mode of storage.[45] Instead, restriction of processing might be sufficient if data subjects have minimal interest in erasure.[2] The French Authority CNIL, in the context of blockchains, suggests that deleting the keyed-hash function's secret key together with the data stored off-chain could be sufficient to fulfill erasure requests as this process renders data on the chain valueless, and it would be highly difficult, if not impossible, to retrieve information.[36] To ensure legal certainty with regard to the implementation of the GDPR, there is a need for guidance at the European level with regard to the meaning of "erasure", and how it can be fulfilled under the GDPR.[2]

Data Protection by Design and Default

The GDPR has set strict principles of personal data protection and obligations on responsible parties and rights for data subjects. However, there should also be a technical infrastructure to support all these and ensure compliance with the GDPR. With such an infrastructure, blockchain may offer great advantages. Taking into account the long-lasting debates around the compatibility of blockchain with the GDPR, it is worth stressing that blockchain is a class of technology, and there is not only one way to design it. With its specific features, blockchain may help achieve some objectives of the GDPR.

GDPR compliance of a blockchain use case, to a significant extent, can be ensured by implementing privacy-preserving features in the design of the blockchain protocol, and this is what Article 25 of the GDPR, by stipulating the principles of data protection by design (which is also called "privacy by design") and by default, requires. As noted by the French Data Protection Authority CNIL, data controllers, according to this principle, are required to select the format and methods without impact on data subjects' rights and freedoms to the greatest extent possible.[36] Although data protection by design and data protection by default principles are sometimes referred to as one, a distinction between the two is made by Article 25 GDPR as follows:

- Data protection by design requires the implementation of appropriate technical and organizational measures, such as pseudonymization, that are designed to implement data protection principles, such as data minimization principle, and to integrate the necessary safeguards into the processing to fulfill the GDPR requirements and protect the right of the data subjects.
- On the other hand, data protection by default requires the implementation of appropriate technical and organizational measures in order to ensure that, by default, only necessary personal data for each specific processing purpose are processed, and that, by default, personal data are not made accessible to others without the individual's intervention to an indefinite number of natural persons.

Especially when combined with off-chain solutions, blockchains can be designed and deployed in a more data protection-enhancing way. In order to comply with the GDPR, blockchain can be used on a layer above databases, and this can allow monitoring transactions on the data exchange and access information while all personal data are stored off the blockchain. Thus, the data stored off-chain will be anchored to the blockchain with a cryptographic reference, and the blockchain will merely be used to keep a record of the processing operations that take place off-chain.[4] The CNIL, in its study to examine how blockchains can be used in the most privacy-preserving way, recommends solutions, in which personal data are processed outside of the blockchain, and only one of the following cryptographic identifiers is stored on the blockchain:

- a commitment of the data;
- a hash generated by a keyed hash function on the data;
- a ciphertext of the data.[36]

As explained previously, even when the personal data are stored off-chain and only anchored to it with one of these cryptographic identifiers, these identifiers will still be classified as personal data. However, it is argued that keeping these public keys on-chain is the key to blockchains' proper functioning and they cannot be further minimized, and, thus, it is seen in compliance with the GDPR to store them as long as the blockchain exists.[36]

The CNIL further notes that the choice of a proper cryptological method to store the data off-chain not only supports risk minimization but also allows data subjects to move closer to an effective exercise of their data protection rights. Erasing the data stored off-chain and the elements enabling their verification will cut off the link with the proof recorded on-chain, and it will be extremely difficult, if not impossible, to retrieve the personal data. In addition, blockchain developers should also take data subjects' rights into account while programming smart contracts and allow data subjects to restrict processing and request human intervention.[36]

It is crucial to note that data protection by design and default approach should be adopted both during the design process of a technological solution and during the processing itself. These include not only technical measures but also organizational and procedural ones. In other words, in addition to the design and operation of technologies, organizational policies and business strategies should be addressed with the purpose of complying with the data protection principles and ensuring the effective implementation of data subject rights. Thus, these measures may take the form of advanced technological solutions – as explained above, training for staff members, or any other appropriate measures.[12]

As there is not any one-size-fits-all methodology, controllers are required to assess the most suitable measures under the particular circumstances in order to ensure effective implementation of the data protection principles and data subject's rights. Putting robust and scalable measures in place is crucial since, in case of an increased risk of non-compliance, it should be possible to scale up the measure in order to achieve effective implementation of the principles and rights.[46] Noteworthy is that data protection impact assessments (DPIAs), regulated under Article 35 GDPR, can be very helpful to assess the risks under certain circumstances and determine the appropriate measures.

Pharmaledger Project

As an example mentioned previously, PharmaLedger establishes a blockchain-enabled platform for various healthcare use cases, with the purpose of creating a digital trust ecosystem in health care.[5] From a perspective of pharmaceutical supply chains, it has a more specific objective of improving patient safety and product traceability by laying the groundwork for the use of blockchain technology and serialization throughout the medicine supply chain. The downstream traceability of completed goods would aid in the collection of important product data, enhancing the option of direct product verification by end-users and patients—something that is currently lacking throughout the whole process. The ability to quickly identify suspected or expired items gives a new degree of transparency that is critical for patient awareness and safety. These additional features will be validated by PharmaLedger through four use cases: eLeaflet, Clinical Supply Chain, Finished Goods Traceability, and Anti-Counterfeiting.[2] Since there may be many different blockchain applications in the context of pharmaceutical supply chains, the PharmaLedger Project will be taken as an example to concretize the explanations made so far.

This approach seems appropriate considering that blockchain is a class of technology still under development, and concrete examples and design can provide more detailed and real-world-based explanations. Furthermore, as highlighted in research managed by the EU Parliament's Scientific Foresight Unit, although regulatory guidance as well as codes of conduct and certification mechanisms could increase the legal certainty regarding how the GDPR could apply to blockchains, this will not always be sufficient to ensure compliance of specific blockchain use cases with the GDPR where there are technical restraints to compliance. It could be possible to find solutions by conducting interdisciplinary research, devising technical and governance remedies, and experimenting with blockchain protocols that could be compliant by design.[22] As an EU-funded project, PharmaLedger aims to provide solutions that could be scalable for other use cases, which may be developed by the healthcare sector in the future, in a way compliant with numerous legal instruments including the GDPR. Thus, examining these solutions offered by the PharmaLedger project could also help to assess to what extent the EU-supported research activities and innovative outcomes are able to fulfill the strategy intended by the EU regulations, which is, in this case, the GDPR.

Overview of the PharmaLedger Architecture

PharmaLedger is designed to be built on a multi-layered hierarchical blockchain solution that is technology agnostic and, so, allows using independent blockchains for different key functions of the platform, such as decentralized identity management, as well as the use cases. The primary objectives of using blockchains are to anchor off-chain data and code and, thus, to be able to replace the blockchain infrastructure without a need to modify application code, and to have greater code and data protection, security, and confidentiality. In this structure, anchoring data only takes place in a hierarchical manner.[2] A high-level, simplified version of the PharmaLedger architecture is illustrated in Figure 1.[2]

Besides the hierarchical blockchain structure, the other core component of PharmaLedger is the concept of OpenDSU (Open Data Sharing Unit). DSUs are stored off-chain as encrypted data blocks and anchored with a hash in a distributed ledger, which is anchored on a parent blockchain. The data on that blockchain are also anchored on the root blockchain with the purpose of inheriting its properties. It is possible to store DSUs anywhere by avoiding the storage provider having control over their content. Private keys, which are used for signing DSU contents and for client-side encryption, allow access to the DSUs. A unique type of cryptographic identifier called KeySSI (Key Self Sovereign Identity) is employed by DSUs, and they function as both keys to decrypt DSUs and self-sovereign identifiers (SSIs) for the elements contained in the DSUs. User-specific data are stored at a DSU component called a "digital wallet," which runs as an application on a smartphone, computer,

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

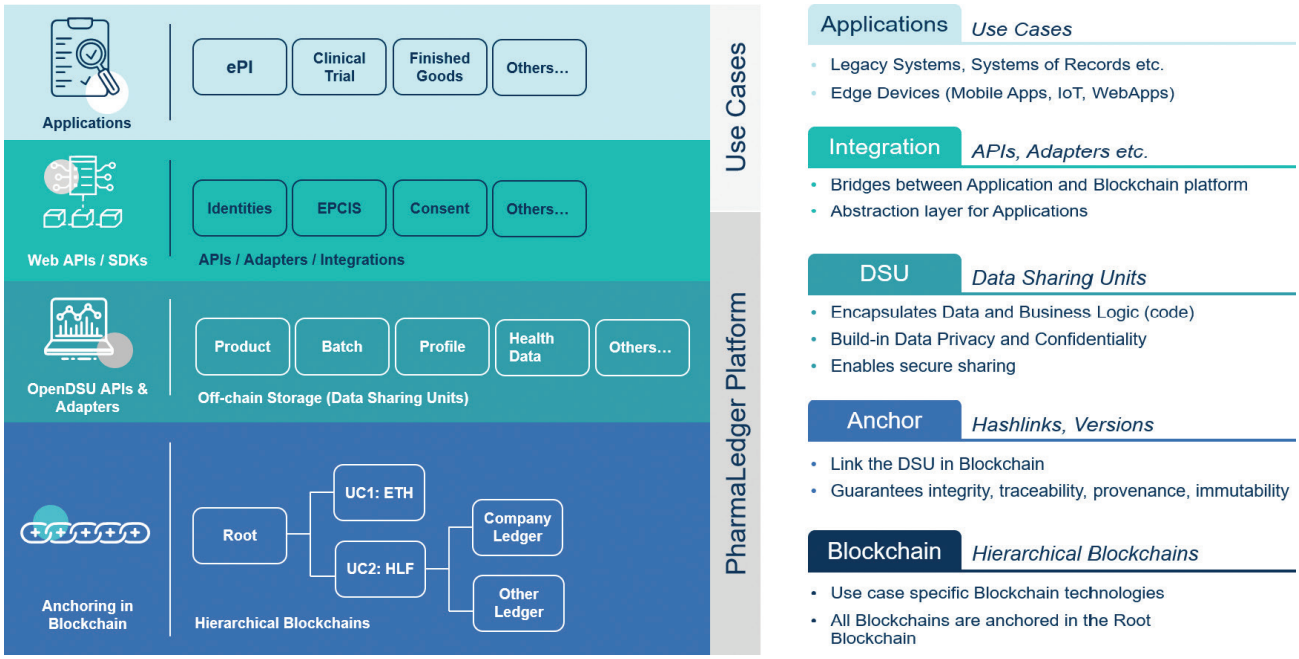

Fig. 1. The layered high-level architecture of the PharmaLedger

or another similar device. It stores keys and certain items such as health information and credentials and controls access to these items, besides communicating with other digital wallets. Therefore, the development of a digital wallet controlled by the user is crucial to achieving the objectives of PharmaLedger.[2] The OpenDSU also eliminates the need for building a specific off-chain storage solution for each different use case/application. As an open standard, this solution can be adopted by different blockchain-based environments.[47]

The highest layer of the PharmaLedger infrastructure, and the closest one to the end-users, is the application layer to which business applications and end-user applications (both mobile and web) belong. While the business applications have an objective of enabling the creation and publication of data on the particular PharmaLedger use case ledger, the end-user applications are meant to allow the end-user to access the DSU storage.[2]

Use Cases in the Pharmaceutical Supply Chain Domain

The PharmaLedger Project has identified eight use cases in three domains, namely, clinical trials, health data, and pharmaceutical supply chains. However, in line with the focus of this paper, only four of them, which are in the context of pharmaceutical supply chains, will be examined. These are eLeaflet (also called, electronic product information, "ePI"), Clinical Supply Chain, Finished Goods Traceability, and Anti-Counterfeiting use cases. These can be briefly explained as follows:

- In the **ePI** use case, the manufacturer creates the package leaflet (also known as Product Information, which contains information that accompanies the medicinal product) in a digital form. Health authorities review and approve the ePI. The manufacturer, then, makes updates to the ePI in this digital form and disseminates it to the end-user, which can be a patient, healthcare practitioner, or healthcare provider.
- The **Anti-Counterfeiting** use case adds additional functionalities and user experience to the ePI use case, in order to create a multi-factor product authentication capability. The initial focus and prioritization of the two use cases are to provide patients with a publicly available smartphone application to easily and anonymously access the electronic leaflet of a chosen medicinal product and check its validity. Patients will not be required to register to use the application. Yet, the application will offer an option to enable certain functionalities, such as geolocation. This functionality will help prioritize anti-falsified medicine efforts for the public good.
- The **Finished Goods Traceability** use case aims to ensure product visibility and status by documenting specific product movements. A degree of certainty about the product's provenance will be offered by the traceability of finished products. This use case will capture all key movements of a product throughout the supply chain, by creating the information flow of shipping finished goods from a manufacturing site via wholesalers and distributors to pharmacies and hospitals. Access to the application will be granted at the

organization level, where individual users (employees) register, and certain information including name, organization, organization type, and access rights (such as administrator, editor, and viewer) will be shown.
- The **Clinical Supply Chain** use case outlines the process of tracking products from initiation of a shipment request to end-use, which can be patient consumption, product return, or product destruction. Although it is out of scope for the Minimum Viable Product (MVP), creating a solution that allows for direct-to-patient track and trace functionality may be considered in the future. This use case begins with the initiation of a shipment request and ends with the reconciliation of an investigational product by the clinical site. Therefore, the standalone mobile application will be targeted at sponsors, distributors, couriers, and sites. Access to the application will be granted upon logging in with the respective credentials of the users.[2]

The possible ways to use blockchain for supply chains are of course not limited to the examples given above. However, the explanations in this section can be a good basis for analogy and, so, useful for other use cases developed by different actors in pharmaceutical supply chains, with regard to compliance with data protection and privacy principles.

Types of Personal Data to be Processed

In the PharmaLedger's Finished Goods Traceability and Clinical Supply Chain use cases, there is likely a very limited amount of personal data required to be processed in order to trace the products. While the data about public or private entities are not classified as personal data, the employees' data will be classified as personal data. Those data may include the names and contact details of the employees involved in the shipments and other related processes. None of these represents particularly sensitive data.

On the other hand, PharmaLedger's ePI use case, where end users can access the product information easily in digital form, and the collection of personal data are not required to achieve the purposes and, thus, should be avoided to comply with the data minimization principle. This is crucial since, for example, creating medical profiles of patients based on the pharmaceutical products of which they accessed the information would involve highly sensitive data and represent serious risks to the rights and freedoms of the end users. The same applies to the Anti-Counterfeiting use case that is being developed by PharmaLedger for the purpose of fighting against falsified medicines.

Another important issue in the Anti-Counterfeiting use case is related to the use of geolocation. Geolocation may result in the identification of an individual, or it may also be combined with other data such as IP address and may serve to identify an individual. For this reason, it is important to take all necessary measures to avoid any permanent personal identifiers (e.g., names, email addresses, social security numbers, any other personal identifiers, or device identifiers) to be combined with geolocation information and data of scanned medicinal products. Otherwise, there may again be serious risks of profiling and inferring health information by unauthorized stakeholders. It is also recommended to give end-users an option to opt-in for sharing geolocation data. Even in the cases where end-users opt-in for it, stakeholders, which are authorized to collect geolocation information, should avoid using fine-grained location information if the purpose can be achieved by sharing broader location information.[2]

Governance of the PharmaLedger Project

The PharmaLedger project is governed by a consortium of 12 pharmaceutical companies and 18 public and private entities, including technical, legal, regulatory, academia, research organizations, and patient representative organizations.[5] The research is divided into various work packages working in close coordination, and each work package and each use case are governed by one public and one private partner. Furthermore, major decisions are taken by majority vote in the general assembly where all partners are represented and have an equal say. Thus, the whole consortium is driving the project together. However, it is important to note that the current setting of the PharmaLedger project is not designed for operating a production platform.[2] The research project will come to an end in December 2022 and in order to ensure the sustainability of the platform that has been developed, and there is a clear need to put a governance model in place for the period after the end of the project. Thus, it would be possible to fulfill the mission of the project – which is to benefit all the stakeholders of the healthcare ecosystem, operate and manage the platform, ensure financial and legal oversight, and make a party accountable for decisions, strategies, and else. For these reasons, the PharmaLedger Association has been established as a not-for-profit Swiss association in early 2022, and it will take over the platform. It is important to highlight that the use cases that reach the production level maturity will be governed by the PharmaLedger Association since the current research project setting does not have the mechanisms in place to ensure quality management and regulatory compliance.

The PharmaLedger Association has been established as minimum viable governance in order to enable the development of Quality Management and Data Protection Management Systems for the highly regulated industry, enable a productive launch of the first PharmaLedger use case, ePI, in the last quarter of 2022, and establish

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

a baseline that enables a more in-depth definition of the future governance model. Thus, the consolidated governance plan, with the details on financials, exploitation, governance, and other fundamentals, is under development. The basis could be making the PharmaLedger Association built on membership fees and having a governance board for decision-making.[4] Nevertheless, there should be further elaborations on how to ensure this association will act in a manner as decentralized as possible.

While creating a single entity with decision-making power over the network seems to be the most straightforward solution to comply with the GDPR, it could be said, from a broader perspective, that this goes against the idea behind blockchains, shifting the power from centralized points of control to decentralized peer networks. When there is one party in control, the trust in the processes could be endangered. Thus, it is crucial to put the right balance between the efforts to achieve compliance and functionalities to increase effectiveness, by also not endangering trust in the network, in blockchain networks creating a single entity responsible for network operation.[4] Although the idea is to limit the role of PharmaLedger Association to act as the coordinator and the policymaker but not as the network operator, this consideration of creating the right balance needs to be addressed in the further elaborations of the post-project governance model.

It should also be noted that PharmaLedger, as a multi-layered blockchain platform including an application layer, brings the capability of determining purposes at the application layer, and blockchains will be used as the underlying infrastructure to which these applications will be anchored. Thus, the entities that determine the purposes at the application layer will qualify as data controllers for their own processing operations. This is also in line with the suggestions of the above-mentioned research managed by the EU Parliament's Scientific Foresight Unit.[22] In other words, the data controller for specific applications to be developed and deployed on the platform might be different from the data controllers for the platform. Each data controller will have a liability limited with its responsibilities and limits of its processing activities.[2] It would be useful to make this clear in the governance model of the multi-layered blockchain platforms like PharmaLedger.

Measures to Comply with the GDPR

As explained previously, there are important factors that are at the roots of the long-lasting debates around the compatibility of the blockchain technologies with the GDPR, but it is also widely argued that with the right design and combination with different technological solutions, blockchains have a great potential to realize the underlying objectives of the GDPR, most prominently giving back individuals control over their personal data. This is only possible by implementing the data protection by design and default principles, which requires putting organizational and technical measures in place from the very beginning of the design process of any new technology which may process personal data. Taking this into account, the PharmaLedger project put these principles at its core and adopted a seven-step process, based on the guidelines developed by the Norwegian Data Protection Authority.[48] As data protection is not a one-off practice but a continuous process, each activity in this approach represents a step leading to the next one in the circle, as illustrated in Figure 2.[12] The involved organizations need to determine which steps should be emphasized and where and when increased effort would be necessary. For the sake of brevity, these steps will not be explained further here, but instead, what technical and organizational measures have been, or can be, taken will be explained.

The first and foremost requirement of data protection by design and default is to meet data protection principles to the greatest extent possible. Thus, any processing of personal data on the PharmaLedger platform is required to be lawful, fair, transparent, and carried out for specified, explicit, and legitimate purposes by minimizing the data processed.[12] At this point, the OpenDSU concept deserves particular attention. The OpenDSU, as an innovative solution, offers data subjects, with smartphone applications "digital wallets," the possibility to manage the personal data stored off-chain and the abilities of other parties to access and process it. With the control over access rights to be granted to the other parties, data subjects can be in better control over their personal data as

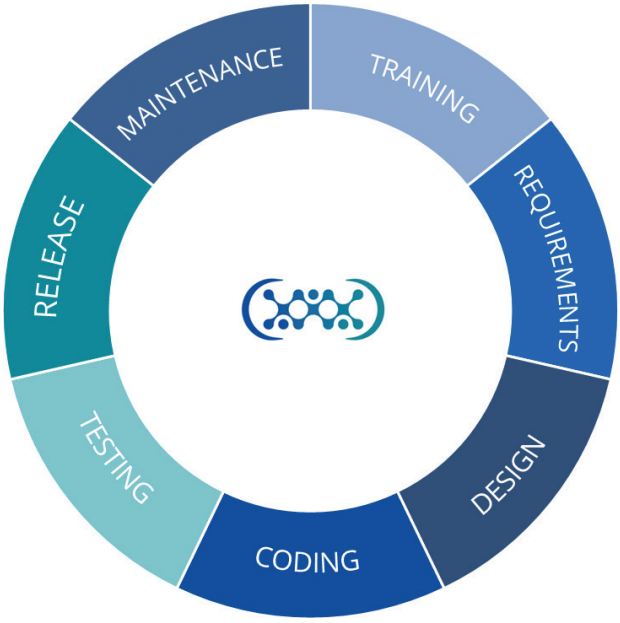

Fig. 2. Data protection by design and by default process in the PharmaLedger project

they decide whether certain information from their digital wallet is shared with requesting parties. By constituting an abstraction layer in the PharmaLedger infrastructure, the OpenDSU offers reusability, interoperability between use cases, and data portability. The blockchain is accessible through digital wallets, which are applications handling the keys. Personal data are not stored on the blockchain but outside the blockchain. This off-chain data storage solution brings an opportunity for more straightforward compliance with the data minimization principle as well as the data subject rights to erasure and rectification.[2]

The PharmaLedger project also adopts self-sovereign identities (SSI), which aim at giving data subjects full control over their digital identities and all identity-related attributes. By having established an Identity Management Task Force (IMTF), the PharmaLedger project takes this technology at its focus and creates digital wallets to store credentials and confidential data and to manage access to the off-chain OpenDSUs. Users will have full freedom over what verifiable claims, which are stored in digital wallets, to share with whichever party users interact with. Blockchain is the technology that allows this identity model to be established. This concept can offer significant data protection and privacy benefits, including:

- Using zero-knowledge proof protocols that do not provide any additional information
- Limiting attributes to the absolute minimum necessity
- Possibility to exchange verifiable claims off-chain via encrypted channels[2]

These concepts of OpenDSU and SSI uphold the GDPR principles of data security and data minimization. The latter is particularly at the heart of the most heated debates on the compatibility between blockchains and the GDPR. These solutions show that blockchain, when appropriately designed and combined with the right technological solutions, could be handy in implementing the GDPR principles and achieving some of its underlying objectives, namely, giving data subjects more control over their data.

Besides the technical design, organizational measures should also be well addressed, particularly in determining the details of the post-project governance structure. Unless the GDPR principles are embedded in the governance model, such as by contractual requirements that need to be agreed on by the future members of the PharmaLedger as a condition of being granted permissions in the permissioned blockchains to be deployed, the technical design will only have a limited impact on ensuring the effective implementation of data protection principles and data subject rights. Many other organizational measures may surely be put in place for this purpose, and this is why an in-depth study taking place in the PharmaLedger project at the time of writing this article is the appropriate approach.

In the PharmaLedger platform, where use cases are not only about pharmaceutical supply chains but also clinical trials and health data, it is necessary to go beyond the above-explained requirements focusing on supply chains and take appropriate measures to protect different sorts of personal data, including highly sensitive health data of patients. If any pharmaceutical supply chain use case is combined with the other use cases, aggregated profiles of patients may be created without these data subjects' knowledge, and this may result in significant breaches of the GDPR. To avoid these kinds of situations, data protection by design, as well as data protection by default, procedures have a role of utmost importance. It is also key, prior to putting these use cases into the market, to conduct DPIAs in order to identify any high risk to the rights and freedoms of data subjects and to mitigate those risks.

The success of the PharmaLedger platform will mostly depend on its wide adoption by numerous actors in the healthcare sector, maturity-achieved launches of the use cases under development as well as the future use cases to be developed, effective quality and data protection management systems, and the final governance structure that will act as the coordinator of and the decision-maker over the platform. While coming to the end of the research project, the efforts put in place by all 29 partners seem to have produced favorable results to design a data protection-enhancing platform that has promises to bring the blockchain's potential into the real world, particularly in pharmaceuticals supply chains.

Conclusions

While pharmaceutical supply chains are complex structures including many different stakeholders, it is also a highly regulated area in the EU. Besides ensuring compliance with the legal and regulatory instruments, creating trust is also key to ensuring effectiveness in these supply chains and protecting public health. This is where blockchains bring a number of promises. However, their potential still has not completely been realized, and especially in the EU, this is closely linked to discussions around how to design and deploy blockchains in compliance with the strict data protection rules under the GDPR as there are long-lasting debates around their, allegedly, conflicting natures.

However, if a blockchain network is developed by adopting strong data protection by design and by default approach under the GDPR, specific features of blockchain may help achieve some objectives of the GDPR, such as data sovereignty, trust in the accuracy of data, better accountability, and data integrity and security, among others. When combined with other technological solutions as in the case of self-sovereign identities, blockchains can provide greater autonomy and control to individuals on their personal data and opportunities to enforce their data subject rights with ease.

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

There is a need for regulatory guidance on how to implement the GDPR in blockchain use cases, but, as in line with the data protection by design approach, new technological solutions can be designed to achieve certain objectives of the GDPR, though not with the mechanisms envisaged by the regulation itself. For this reason, this paper has examined whether PharmaLedger, an EU-funded innovative research project, has the right mechanisms to be seen as a blueprint for pharmaceutical supply chains using blockchains. It is true that this project has an important potential, but much will depend on the details to be determined, such as the governance structure of the platform. Nevertheless, it is a good example to show that there is a clear technological shift toward more GDPR-compliant blockchain designs.

Funding Statement

PharmaLedger project is funded through the Innovative Medicines Initiative (IMI) 2 Joint Undertaking and listed under grant agreement No.853992. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and the European Federation of Pharmaceutical Industries and Associations (EFPIA). A part of the budget of this project is dedicated to the dissemination of the results of the research being conducted. This research has received no external funding. The funders had no role in the study design, data collection, and analysis, decision to publish, or preparation of the manuscript.

Financial and non-Financial Relationship and Activities

As the representative of KU Leuven in the consortium of the PharmaLedger project, the author acts as the co-leader for the work package on the Regulatory, Legal, and Data Privacy Framework. In this capacity, his role is to provide academic research in order to guide the consortium regarding the applicable ethical, legal, and regulatory frame works.

Contributors

The author is responsible for the content of this article.

References

1. Clauson K, Breeden E, Davidson C, Mackey T. Leveraging blockchain technology to enhance supply chain management in healthcare. Blockchain Healthc Today. 2018;1. https://doi.org/10.30953/bhty.v1.20
2. Georgiev N, Yaşar B, Inari Castella S, et al. PharmaLedger deliverable 5.2: in-depth ethical and legal study. 2021. Available from: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e26c7cd9&appId=PPGMS [cited 28 February 2022].
3. Finck M. Blockchains and data protection in the European Union. Eur Data Protect Law Rev. 2018;4(1):17–35. https://doi.org/10.21552/edpl/2018/1/6
4. Livitckaia K, Charles W, Larrañaga Piedra U, Niemerg M, Hasselgren A, Papadopoulou E. Blockchain application in healthcare sector. EU Blockchain Observatory and Forum; 2022. Available from: https://www.eublockchainforum.eu/sites/default/files/reports/eubof_healthcare_2022_FINAL_pdf.pdf [cited 28 February 2022].
5. PharmaLedger. 2022. Available from: https://pharmaledger.eu/ [cited 28 February 2022].
6. Schöner M, Kourouklis D, Sandner P, Gonzalez E, Förster J. Blockchain technology in the pharmaceutical industry. Frankfurt: Frankfurt School Blockchain Center; 2017. Available from: https://philippsandner.medium.com/blockchain-technology-in-the-pharmaceutical-industry-3a3229251afd [cited 28 February 2022].
7. Arviem AG. Quick guide to pharma supply chain visibility. Arviem AG; 2017. Available from: https://arviem.com/wordpress/wp-content/uploads/2017/10/Quick-Guide-to-Pharma-Supply-Chain-Traceability.pdf [cited 28 February 2022].
8. Hurley J. Creating a transparent supply chain for prescription drugs—InsideSources. InsideSources. 2017. Available from: https://insidesources.com/creating-transparent-supply-chain-prescription-drugs/ [cited 2 March 2022].
9. European Commission (EC). Pharmaceutical strategy for Europe. EC; 2020. Available from: https://ec.europa.eu/health/system/files/2021-02/pharma-strategy_report_en_0.pdf [cited 4 March 2022].
10. Bagozzi D, Lindmeier C. 1 in 10 medical products in developing countries is substandard or falsified. WHO; 2017. Available from: https://www.who.int/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified [cited 4 March 2022].
11. McCauley A. Why big pharma is betting on blockchain. Harvard Business Review. 2020. Available from: https://hbr.org/2020/05/why-big-pharma-is-betting-on-blockchain [cited 7 March 2022].
12. Georgiev N, Van Der Eycken D, Castella S, et al. PharmaLedger deliverable 5.1: ethical and legal inventory. 2020. Available from: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5d41d340b&appId=PPGMS [cited 9 March 2022].
13. Directive 2001/83/EC of the European Parliament and of the Council on the Community code relating to medicinal products for human use (November 6, 2011). Available from: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/directive-2001/83/ec-european-parliament-council-6-november-2001-community-code-relating-medicinal-products-human-use_en.pdf [cited 4 May 2022].
14. Directive 2003/94/EC laying down the principles and guidelines of good manufacturing practice in respect of medicinal products for human use and investigational medicinal products for human use (October 8, 2003). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:262:0022:0026:en:PDF [cited 4 May 2022].
15. Directive 2011/62/EU of the European Parliament and of the Council amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products (Falsified Medicines Directive) (June 8, 2011). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0074:0087:EN:PDF [cited 4 May 2022].
16. Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health (CETS No. 211) (MEDICRIME Convention) (2011). Available from: https://rm.coe.int/168008482f [cited 4 May 2022].

17. Commission Delegated Regulation (EU) 2016/161 supplementing Directive 2001/83/EC of the European Parliament and of the Council by laying down detailed rules for the safety features appearing on the packaging of medicinal products for human use (October 2, 2015). Available from: https://health.ec.europa.eu/system/files/2016-11/reg_2016_161_en_0.pdf [cited 4 May 2022].
18. Regulation 2020/1056 on electronic freight transport information (July 15, 2020). Available from: https://eur-lex.europa.eu/eli/reg/2020/1056/oj [cited 4 May 2022].
19. Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency (March 31, 2014). Available from: https://health.ec.europa.eu/system/files/2016-11/reg_2004_726_en_0.pdf [cited 20 April 2022].
20. Ciapponi A, Donato M, Gülmezoglu A, Alconada T, Bardach A. Mobile apps for detecting falsified and substandard drugs: a systematic review. PLoS One. 2021;16(2):e0246061. https://doi.org/10.1371/journal.pone.0246061
21. Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR) (April 27, 2016). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [cited 20 April 2022].
22. European Parliament, Directorate-General for Parliamentary Research Services, Finck M. Blockchain and the general data protection regulation: can distributed ledgers be squared with European data protection law? Publications Office; 2019. https://doi.org/10.2861/535
23. EU Charter of Fundamental Rights. (October 26, 2012). Available from: https://fra.europa.eu/en/eu-charter [cited 20 April 2022].
24. Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights. Handbook on European data protection law. Luxembourg: Publications Office of the European Union; 2018. https://doi.org/10.2811/343461
25. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) (October 24, 1995). 31995L0046 - EN - EUR-Lex - European Union. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex-%3A12016P%2FTXT [cited 20 April 2022].
26. Center for Global Enterprise, Slaughter and May, Cravath, Swaine & Moore LLP. March of the blocks—GDPR and the blockchain. Digital Supply Chain Institute; 2019. Available from: https://www.dscinstitute.org/assets/documents/GDPR-and-Blockchain-March-of-Blocks.pdf [cited 14 March 2022].
27. Gaur V, Gaiha A. Building a transparent supply chain. Harvard Business Review. 2020. Available from: https://hbr.org/2020/05/building-a-transparent-supply-chain [cited 15 March 2022].
28. Article 29 Data Protection Working Party (WP29). "Guidelines on the right to data portability" 16/EN WP 242 rev.01. European Commission (EC); 2017. Available from: https://ec.europa.eu/newsroom/article29/items/611233 [cited 16 March 2022].
29. Mainelli M. Blockchain could help us reclaim control of our personal data. Harvard Business Review. 2017. Available from: https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data [cited 17 March 2022].
30. Lyons T, Courcelas L, Timsit K. Blockchain and digital identity. EU Blockchain Observatory and Forum; 2019. Available from: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf [cited 18 July 2022].
31. Zyskind G, Nathan O, Pentland A. Decentralizing privacy: using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops. 2015. https://doi.org/10.1109/SPW.2015.27
32. Article 29 Data Protection Working Party (WP29). "Opinion 04/2014 on anonymisation techniques" (2014) 0829/14/EN. European Commission (EC); 2014. Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [cited 18 March 2022].
33. Lyons T, Courcelas L, Timsit K. Blockchain and the GDPR. EU Blockchain Observatory and Forum; 2018. Available from: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf [cited 21 March 2022].
34. Moerel L. Blockchain & data protection... and why they are not on a collision course. Eur Rev Priv Law. 2018;26(6):825–51. https://doi.org/10.54648/erpl2018057
35. Moerel L, Storm M. Blockchain can both enhance and undermine compliance but is not inherently at odds with EU privacy laws. J Invest Compl. 2021;22(2):122–32. https://doi.org/10.1108/JOIC-10-2020-0037
36. Commission Nationale Informatique et Libertés (CNIL). Solutions for a responsible use of the blockchain in the context of personal data. CNIL; 2018. Available from: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf [cited 22 March 2022].
37. *Schrems II* [2020] Case C-311/18 (Court of Justice of the European Union). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 [cited 20 April 2022].
38. European Data Protection Board (EDPB). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. EDPB; 2021. Available from: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en [cited 26 April 2022].
39. European Commission. Standard contractual clauses (SCC). European Commission; 2022. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [cited 18 July 2022].
40. Zetoony D. What exactly is a "transfer impact assessment" (TIA), and where the heck did it come from? Data Privacy Dish. 2022. Available from: https://www.gtlaw-dataprivacydish.com/2022/03/what-exactly-is-a-transfer-impact-assessment-tia-and-where-the-heck-did-it-come-from/ [cited 26 April 2022].
41. Neuburger J, Choy W. Practical law. 2019;(3). Available from: https://content.next.westlaw.com/practical-law/the-journal/practical-law-the-journal-transactions-business-july-aug-2019?transitionType=Default&contextData=(sc.Default)&navId=6105953F4C405848E6F2A965BE757D72 [cited 23 March 2022].
42. Bacon J, Michels J, Millard C, Singh J. Blockchain demystified. Queen Mary University of London School of Law; 2017. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218 [cited 25 March 2022].
43. Berberich M, Steiner M. Blockchain technology and the GDPR—how to reconcile privacy and distributed ledgers? Eur Data Protect Law Rev. 2016;2(3):422–6. https://doi.org/10.21552/EDPL/2016/3/21

Citation: Blockchain in Healthcare Today 2022, **5**: 232 - http://dx.doi.org/10.30953/bhty.v5.232

44. Information Commissioner Office (ICO). Deleting personal data. ICO. Available from: https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf [cited 28 March 2022].
45. Section 35 of the Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680. Available from: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1661524539706 [cited 20 April 2022].
46. European Data Protection Board (EDPB). Guidelines 4/2019 on article 25 data protection by design and by default. EDPB; 2019. Available from: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf [cited 29 March 2022].
47. OpenDSU. 2022. Available from: https://opendsu.com/ [cited 4 April 2022].
48. Software development with data protection by design and by default. Datatilsynet. 2022. Available from: https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true [cited 8 April 2022].