Renata Hrecska-Kovacs

Health Law Implications of the Use of Blockchain Technology

Blockchain technology offers many opportunities in healthcare, starting from the efficient management of health data, the prevention of privacy violations, the enhancement of interoperability, the more efficient performance of prescribed and necessary medical treatments, the traceability of drugs and prescriptions, the drug supply chain, and all employees to enhanced control of an IoT device. For the legislator, technological development is a constant challenge – in this field, the general expectation that the law should anticipate problems and settle life situations before they arise is almost impossible to achieve. The information society – and thus blockchain technology – imposes constantly renewed legislative tasks on professionals. The distributed data storage nature of the blockchain, the ownership issues of data records, and the establishment and maintenance of access guarantees are constant regulatory challenges.*

* Rejeb, Abderahman, Horst Treiblmaie, Karim Rejeb, Suhaiza Zailani, „Blockchain Research in Healthcare: A Bibliometric Review and Current Research Trends" Journal of Data, Information and Management, No. 3 (2021): 109–124. https://doi.org/10.1007/s42488-021-00046-2. [accessed: 15.09.2022].

Renata Hrecska-Kovacs

PhD in law, LLM
Ferenc Mádl Institute of Comparative Law

ORCID – 0009-0006-0764-5540

e-mail: dr.h.renata@gmail.com

Key words:
blockchain, data protection, GDPR, healthcare, lex cryptography

https://doi.org/10.36128/priw.vi44.541

1. Introduction

Code is the human-made architecture of cyberspace; thus, technology can control individual behavior. It imposes systematic limits on the individual's behavior in an artificial environment. Thus we can apostrophize the code designer as the rule maker of the technological environment – such as the Internet or digital platforms[1]. The nature of blockchain technology makes regulation through code extremely powerful and decisive: the tamper-proof nature of the distributed ledger and the possibility to automate transactions

[1] Georgios Dimitropoulos, „The Law of Blockchain" *Washington Law Review*, No. 3 (2020): 1117-1192.

make the so-called *lex cryptographia*[2] an effective regulatory code. At the same time, a significant circumstance from the point of view of our topic is that the *lex cryptographia* is also subject to external regulation – consisting of actual legislation – which it must fully comply with during its operation. The relationship between the two regulatory levels can be determined not by substitution but by supplementing each other. In this study, based on the international literature and various case studies, I examine the conditions under which blockchain technology can be used in the healthcare provider system and the legal implications of this in everyday life.

2. The concept of the blockchain and its introduction to healthcare

The primary goal of blockchain technology is to achieve transparent data provision through a distributed database (*ledger*) that contains a time stamp and a link to a previous block. As an immutable, single-write system, the advantage is that the information contained in it cannot be altered retroactively, and there is no central data register[3], as a result of which the transactions between the parties can be tracked transparently, authentically, and permanently. The network updates itself regularly, approximately every ten

[2] The *lex cryptographia* is and algorithmic set of rules, which can be defined as a system of rules managed through smart contracts and decentralized networks. For the concept see among others Katrin Becker, „Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries" *Law and Critique*, 33 (2022): 113-130. https://link.springer.com/article/10.1007/s10978-021-09317-8. [accessed: 15.09.2022]; Aaron Wright, Primavera De Filippi, „Decentralized Blockchain Technology and the Rise of Lex Cryptographia" *Social Science Research Network*, 10 March 2015. http://dx.doi.org/10.2139/ssrn.2580664. [accessed: 15.09.2022]; Sai Agnikhotram, Antonios Kouroutakis, „Doctrinal Challenges for the Legality of Smart Contracts: Lex Cryptographia or a New, Smart Way to Contract" *Journal of High Technology Law* No. 2 (2019): 300-328; Thibault Schrepel, „Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia" *Social Science Research Network*, 12 November 2019. https://ssrn.com/abstract=3485436. [accessed: 15.09.2022].

[3] The advantage of the lack of a central register is primarily manifested in the fact that, thanks to the distributed ledger system, any small unit of the data set can be changed using an enormous amount of computing capacity, since copying the data requires overwriting the entire network. (see *Mi az a blokklánc?* Átfogó útmutató és *jövőbeli alkalmazási területei*. https://www.bitcoinbazis.hu/utmutato/blokklanc-utmutato/. [accessed: 15.09.2022])

minutes, and reconciles each transaction, so the data can always be kept up--to-date[4].

At the same time, technology should not be overestimated: it is a well-known saying that if your only tool is a hammer, you tend to see every problem as a nail. The blockchain is not a universal solution for all data and information-related issues: its primary field may be where the need for change tracking plays an increased role[5]. Overall, it is necessary to assess when and in which cases blockchain technology can be used most effectively, taking care of the systems' automation and selecting the appropriate permission system.

Blockchain can be a suitable solution if four prerequisites exist: on the one hand, several parties must generate transactions that change information in a shared database; the parties must also trust that the transactions are valid; it is also a prerequisite that the inclusion of any intermediary[6] in the data transmission chain would result in a loss of efficiency or unreliable data provision; and enhanced security should be required to ensure the integrity of the system[7].

[4] For a simple description of how the blockchain works, see among others Robert A Stines, „Blockchain 101: A Lawyer's (Brief) Guide" *Tort-Source*, Spring (2019): 14-15; Dave Berson, Susan Berson, „Blockchain Law 101: Understanding Blockchain Technology and the Applicable Law" *Journal of the Kansas Bar Association*, No. 2 (2019): 40-43.

[5] On this issue see, for example, Peter Nadimi, Samuel G. Korver, Zach Smolinski, Lauren M. W. Steinhaeuser, Corey Bieber, „Practicing Blockchain Law [comments] Panel III" *John Marshall Journal of Information Technology and Privacy Law*, No. 1 (2019): 57.

[6] Third parties who are capable of checking transactions on the network are called intermediaries. Although blockchain technology can achieve full automation in the field of cryptocurrencies, it is not completely the case in other areas of use. Currently, the literature generally holds that in the case of transactions subject to a verification obligation, it will probably never be completely avoidable to involve a reliable third party to conduct the necessary auditing activity – e.g. if blockchain technology is used to conduct elections, it may be necessary to verify that it is real people started a real transaction on the network. See more Nathan Reiff, „Blockchain won't cut out intermediaries after all" *Investopedia*, 27 October 2011. https://www.investopedia.com/tech/blockchain-wont-cut-out-intermediaries-after-all/. [accessed: 15.09.2022].

[7] R. J. Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai, „Blockchain: Opportunities for Health Care" *Deloitte*, August (2016): 2. https://www2.deloitte.com/content/

Currently, blockchains are primarily used in the cryptocurrency market. Still, they also significantly facilitate work processes in political elections, authentication and authorization procedures, digital content storage and sharing, network infrastructure, and application development. Healthcare is no exception to this, where technology simplifies the management of patient or supply chain-related data.

Suppose it has been proven that building a blockchain network under particular circumstances increases real efficiency or security. In that case, it is also necessary to decide for which motives the solution will be applied: we can think of two primary uses, so we can use the blockchain to verify and authenticate information or transfer values. For example, the system can check the patients' digital identity, genetic data, or medical history in the first case. In the second case, organizations can use the technology to transact value, such as cryptocurrencies or intellectual property rights[8].

In the third stage of the blockchain frameworks' decision-making process, organizations can strengthen their system with smart contracts, which are automatically executed when conditions are met. With the help of the necessary algorithms, the conditions can be customized entirely, i.e., it can be determined when values need to be changed, information to be transmitted, or events need to be triggered. This solution is one of the foundations for applying the blockchain in healthcare, subject to prior authorizations and the automatic processing of claims arising from care service.

Finally, the technology user must decide whether to operate a permissioned or permissionless network. In healthcare, the former is more beneficial since, in this case, only a predetermined group can access the network; it is not available to the public. At the same time, the exact type of blockchain protocol must also be determined, and it must also be chosen in light of the purpose of the network and how many users will be able to access it[9].

In the health sector, we can identify many application areas where the use of blockchain can bring benefits: thus, above all, the technology can be exploited most effectively from the point of view[10] of interoperable medical history databases, patient records, healthcare smart contracts, and clinical

dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf. [accessed: 15.09.2022].

[8] Krawiec et al., *Blockchain: Opportunities*, 3.

[9] Krawiec et al., *Blockchain: Opportunities,* 3.

[10] Christian Dierks, *Legal aspects of blockchains in healthcare.* Presentation. Health in the Digital Society – Digital Society for Health, 16-18 October 2017, Tallin, Estonia.

research[11]. Research into the effective use of blockchain in healthcare has been ongoing in the United States of America for some time. Still, geographically, we find closer to us the state that was the first in the world to be able to incorporate blockchain into the practice of the healthcare service scene on a national level: the Estonian E-Health Foundation (Tervise ja Healou Infosüsteemide Keskus) launched a development project in 2016, the aim of which is to protect patients' health records by using blockchain technology in the archiving of activity logs[12]. With blockchain, it is not protected state records but the log files that record all the data processing activities performed on those records.

An archive or ledger with a backbone based on blockchain technology can record and timestamp each access to or change in the patient's electronic records. Cryptographic hash functions create an immutable audit trail that can be traced. The technology also guarantees that service providers always use the latest version of the record. In the case of Estonia, a private digital ledger has been integrated into the E-Health Foundations' ledger to record and monitor patients' health data. The goal was to make the stored data accessible in real-time and intact and for administrators to detect potential violations and take immediate action to limit the damage. An important detail

[11] For example, according to Interpol reports, the counterfeiting of medicines is a serious threat in today's pharmaceutical trade, which can occur in reduced or ineffective active ingredients, or even in the use of particularly harmful components. (See Interpol, *Fake Medicines.* https://www.interpol.int/Crimes/Illicit-goods/Shop-safely/Fake-medicines. [accessed: 15.09.2022]). The joint solution of DHL and Accentura helps to reduce this phenomenon, which uses blockchain technology to register the path of medicines from manufacturers through warehouses and pharmacies to hospitals and clinics. (see DHL. *DHL and Accenture Unlock the Power of Blockchain in Logistics,* Bonn: Germany, 03/12/2018. https://www.dhl.com/global-en/home/press/press-archive/2018/dhl-and-accenture-unlock-the-power-of-blockchain-in-logistics.html. [accessed: 15.09.2022]). Blockchain, as an indelible, reliable ledger, not only protects patients from life-threatening fraud, but also reduces costs. (Gábor Móray, „Mi az a blokklánc technológia és milyen lehetőségeket kínál?" *Computerworld*, 28 October 2020. https://computerworld.hu/tech/mi-az-a-blokklanc-technologia-es-milyen-lehetosegeket-kinal-285890.html. [accessed: 15.09.2022]).

[12] Taavi Einaste, „Blockchain and healthcare: the Estonian experience" *E-Estonia*, 26 February 2018. https://e-estonia.com/blockchain-healthcare-estonian-experience/. [accessed: 15.09.2022]; and the longer version of the article on https://nortal.com/blog/blockchain-healthcare-estonia/. [accessed: 15.09.2022].

in this issue is that the technology effectively prevents potentially harmful electronic intrusion[13].

2.1. Operational issues underpinning the use of blockchain

Not all processes, therefore, require the use of blockchain. On the other hand, this solution can play an important role in cases where the system has multiple actors and information exchange between these actors is required: this category includes, for example, the relationship between the social security system, health care facilities, and the patients. Trust and security play a significant role in this multilateral legal relationship, so achieving the most controlled framework to share health data[14]is necessary.

According to Deloittes' US-related research in 2016[15], healthcare information exchange networks generally have to deal with six main points. The research aims to analyze the American *Health Information Exchanges* service, so it recommends using the blockchain to solve the technological problems that arise there; however, in my opinion, certain question elements appear universally in the healthcare industry. I would summarize them as follows:

– How can a secure network be created by end-to-end sharing and precisely recorded exchanged data?
– How can transaction costs be reduced in terms of sharing data?
– How can synchronization between patient identifiers be achieved while securing patient data?
– How can record interoperability be achieved if the system uses different data standards?
– How can the limited access to the populations' health data be counterbalanced if the system does not belong to the scope of integrated registration sources?
– How can different protocols and licenses prevent healthcare facilities from accessing patient data on time?

Blockchain technology offers good solutions to these issues, as the trust-supporting network is given if all participants can access the distributed ledger to maintain a secure exchange without the involvement of any intermediary partner. Reducing the number of actors and near-real-time processing also reduces transaction costs, and guarantees institutions can make patient care decisions with up-to-date information.

[13] See https://nortal.com/blog/blockchain-healthcare-estonia/. [accessed: 15.09.2022].

[14] Zoltán Árpási, „A blokklánc alkalmazásának lehetőségei az egészségügyben" *Cryptofalka*, 29 December 2019. https://cryptofalka.hu/blokklanc-egeszsegugyi-alkalmazasa/. [accessed: 15.09.2022].

[15] Krawiecz et al., *Blockchain: Opportunities*.

Smart contracts create a consistent rules-based method of accessing patient data that can be authorized for healthcare organizations. Overall, a distributed patient digital identity framework that uses cryptographically protected private and public keys creates a unique, more secure way to protect patient identities[16].

In healthcare, it is also important that the data is secured against external attacks. Blockchain technology is based on asymmetric encryption (see point 3), so the potential hacking of a single patient's private key does not compromise the network, as an attacker has to hack each user separately to obtain unique private keys for identifiable valuable information to reach. In an era of permieter firewall attacks[17] and ransomware, an effective asynchronous encryption process protects patient identities within organizations[18].

2.2. Types of patient data stored on the blockchain

Healthcare service organizations provide different services to patients, and the related data is stored in the existing IT system of the institutions. This includes, among other things, the patients' public identification number, based on which the given person cannot be identified. Still, the number and related data fields can be placed on the blockchain. This creates a secure but easily searchable database. An important feature is that personal data cannot be identified, but useful analyzes can be made based on demographic characteristics (gender, age, illness).

At the same time, accessing the database formed as part of the procedure is not the main goal but rather a useful result of the technology[19] through which the prepared analyzes can significantly combat diseases. The main advantage of data stored on the blockchain is that the patient, possessing his private key, can share his healthcare data and medical history with whomever he wishes. On the other hand, those who did not receive access to the information still only see a set of data that can be organized based on demographic criteria (point 2.4).

Regarding the data stored on the blockchain, it is important to see what kind of grouping we should consider when dealing with data management. Patient data can be divided into two broad categories: on the one hand, we distinguish between standardized information, which practically

[16] Krawiecz et al., *Blockchain: Opportunities*, 1.

[17] A perimeter firewall is a security application that protects the boundary between a private network and a public network. Its purpose is to prevent unwanted or suspicious data traffic on the network. A typical practical example of its application is when an employer does not want employees to access social media and blocks access to these sites.

[18] Krawiecz et al., *Blockchain: Opportunities*, 7.

[19] Árpási, *A blokklánc alkalmazásának lehetőségei*.

represents patient data regarding sex, age, immunization level, and type of care and is unsuitable for identifying persons or continuing treatment. These data can be viewed without an intervening waiting time and retrieved from the network.

The other group includes actual, detailed health records, available as notes, pictures, genetic maps, etc. These data take up much storage space, so they are not placed as related data on the blockchain network but in other external databases. In this case, a link is recorded on the blockchain, which, when activated, takes the data requester to the actual documentation.

Overall, healthcare providers typically store financial and transactional reports, declarations of consent, clinical examination results, measurement results, treatment and medical histories, and other personal data of patients on the two types of layers. Some of the data is stored by the service provider itself, some by the patient[20], and the service providers amongst each other share some.

3. Legal issues induced by technical development

In connection with the blockchain, data protection issues primarily arise, which makes it difficult to assess the issue, because it is easy to happen that ledgers fall under different jurisdictions, so the GDPR[21], which functions as a basic reference point in the European Union, may not apply to the entire chain. For example, data controllers or data processors that do not have a place of business in the EU do not, as a general rule, fall under the scope of the regulation if they only collect personal data from the territory of the European Union but if, in addition, their business activities are (also) directed to the European Union[22].

If the GDPR is applicable, then legal requirements also exist concerning the blockchain, according to which, on the one hand, it should be

[20] The data stored by the patient means primarily the results of function tests registered by portable diagnostic devices (e.g., vital parameters such as blood pressure, pulse, temperature, breathing characteristics, etc.), which are not accessible to the healthcare provider until they are transmitted.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation, GDPR).

[22] See GDPR (23). Based on the following (24) paragraph, a service provider falls under the scope of the regulation only due to the fact of data management or data processing, if its activity is related to the monitoring of the behavior of legal entities within the Union.

identified where exactly the data is located. The right to deletion should be ensured. Technologically, however, it is not possible to guarantee the right to be forgotten within the blockchain since, on the one hand, the data cannot be located. On the other hand, the main merit of the solution is precisely based on data traceability.

I note here that if we want to protect anonymized[23] data stored on the blockchain, then the scope of the GDPR does not cover this issue since, in the event of data loss or modification, privacy rights are not violated, but primarily property rights issues arise. At the same time, although blockchains and GDPR are conceptually incompatible at first sight, according to EU law, stored data is considered personal data even if the data is encrypted or hashed. Therefore, the cryptographically modified data stored in the distributed ledger is subject to the GDPR[24].

3.1. Exercising the right to be forgotten

To be able to handle any data built into the blockchain legally despite a deletion request, the data controller or data processor must indicate a reason recognized by the GDPR as the purpose of data storage. A good example is a company's accounting documentation, in which the customers' invoices can be found together with their data. In such a case, even if the customer requests the deletion of his data, the service provider cannot do this due to the tax legal environment[25].

However, I would like to emphasize that technological barriers do not legitimize the denial of the deletion request of a natural person affected by the management or processing of their data in the GDPR. Similarly to the GDPR, the issue is regulated outside of Europe, for example, by the California Consumer Privacy Act, which does not recognize the mentioned exception despite the different legal system and social structure[26].

[23] Pursuant to (26) paragraph of the GDPR, by anonymized data we mean information that relates to an unidentified or unidentifiable natural person, as well as personal data that has been anonymized in such a way that the person concerned cannot or can no longer be identified.

[24] Michèle Finck, „Blockchains and Data Protection in the European Union" *European Data Protection Law Review*, No. 1 (2018): 17-35. https://edpl.lexxion.eu/article/edpl/2018/1/6/display/html. [accessed: 15.09.2022].

[25] See Corey Bieber's thoughts on the already quoted conference (Nadimi et al. „Practicing Blockchain Law", 60).

[26] California Legislative Information. *Civil Code*. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. [accessed: 15.09.2022].

3.2. Data controllers and data processors

In light of literature and practice, blockchain poses questions and demands specific answers. We cannot forget, for example, the conceptual problem that must be fundamentally resolved: if we work with many nodes, it is unclear which actor qualifies as a data controller, i.e., to whom the legal obligations apply. I agree with the French data protection authority (Commission Nationale de l'Informatique et des Libertés, CNIL) [27] that the parties that have the right to overwrite the chain and send the data for verification are all considered data controllers.

Groups may manage data. A good example is when a blockchain network is built between a parent company and its subsidiaries, and the nodes are the companies themselves. In such cases, it is worth creating a legal entity or appointing a person within the groups who will be given the status of the data controller and have the competence to decide on issues of responsibility. Based on Article 26 of the GDPR, in the opposite case, all group members share the responsibility because they are considered joint controllers.

Regarding data processors, the blockchain network does not impose special requirements, i.e., we follow the general dogma of the GDPR when we define it as a natural or legal person, public authority, agency, or any other institution that processes personal data on behalf of the data controller[28].

Based on the principle of data minimisation, the data controller can only collect and process the most necessary data while maintaining the time limits required by the legal environment.

3.3. Data life cycle

Three phases of personal data management can be separated and implemented almost without exception during data management. First, we place the data in the active database, and this is the time required to achieve the purpose of justifying data collection/recording (the purpose of data management). For example, the human resources department of a given company keeps the data of job applicants for a maximum of two years (unless the applicant requests their deletion). The data is easily accessible in the immediate work environment for the operational departments responsible for this processing.

In the interim archiving period, the personal data are no longer used to achieve the intended purpose (they are available as closed files). However, they still have an administrative interest in their preservation (e.g., management of a possible dispute, etc.) or must be preserved to fulfill a legal

[27] CNIL, *Solutions for a Responsible use of the Blockchain in the Context of Personal Data*, September 2018; https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf. [accessed: 15.09.2022].

[28] See GDPR Article 4, paragraph (8).

obligation (e.g., invoicing data must be kept for five to ten years under the legislation on trade and taxation, even if the person concerned is no longer a customer). In justified cases, authorized persons can view the data during this period.

In the case of permanent archiving, we keep certain data due to their value and future usability; the same applies to their access, as we said in the case of interim archiving. Unlike active database storage, the last two steps do not appear systematically and in every case. Their necessity must be assessed for each processing.

However, under the scope of the GDPR, it must be taken into account that the data must be stored in a form that allows the identification of the data subjects only for the time necessary to achieve the goals of personal data management. Personal data may be stored for a longer period only if the personal data will be processed for archiving in the public interest, for scientific and historical research purposes, or for statistical purposes, also taking into account the implementation of the appropriate technical and organizational measures prescribed in the Regulation to protect the rights and freedoms of the data subjects. The GDPR calls this storage limitation[29].

3.4. Commitment scheme for data protection

It is well-known about the blockchain network that the transparency of the stored data is guaranteed. This is exactly the purpose of technology. At the same time, using encryption systems can help ensure that, although the data can still be found in the system, its visibility is significantly restricted by the so-called commitment scheme. Based on this, the sender commits to a certain value initially hidden from the recipient. Later, the sender can reveal the value to the recipient but can no longer change its content.

Knowing the protocol is important because the GDPR stipulates the principle of data saving or minimization, which must be appropriate and relevant for data management and limited to what is necessary[30]. Based on the commitment scheme, the only thing visible on the blockchain network is a data package; however, the data controller does not have access to its exact content until the data owner authorizes this with his public key. Translated into practice: although the patients' data is available to the institutions and service providers connected to the blockchain network, at the same time, to query the specific health records, the clients' approval is required (see what was written previously in point 1.2)[31].

[29] See GDPR Article 5, paragraph (1), point e).

[30] See GDPR Article 5, paragraph (1), point c).

[31] It is also true here that the rules of authorization and legal succession apply to the procedural actions taken by the client (e.g. in the case of statements made by minors and heirs).

3.5. Smart contracts

In the case of smart contracts, a legal transaction is created between anonymous parties: the contracts work by following the instructions coded on the given blockchain. These instructions are encrypted locally at the data source; the system does not use an unlocking key. The system performs the programmed actions automatically, without the involvement of a third party, if the predefined conditions are met. The behavior of each party can be checked independently, including the correctness of the result of the entire calculation and the fulfillment of data protection requirements. The blockchain is updated when the transaction is completed[32].

One significant difference between smart and standard contracts is the execution and termination mechanism. Smart contracts enforce obligations through autonomous code, i.e., a strict and formal programming language where nodes in the underlying network distribute the code. This makes it difficult to terminate smart contracts unless such termination is properly coded into the software. Additionally, smart contracts are more dynamic than traditional legal contracts because performance obligations can be adjusted over time through trusted third-party sources, the so-called oracles[33]. However, this latter point is questionable, as many legal contracts are potentially

[32] Marco Rauland, *Are You Smart Enough? Blockchain & Smart Contract Applications in Pharma*, 10.02.2022; https://pharmaboardroom.com/articles/are-you-smart-enough-blockchain-smart-contract-applications-in-pharma/. [accessed: 15.09.2022].

[33] The oracle is a bridge between the blockchain and the real world. They act as on-chain APIs that can be queried to call information into smart contracts. This can be anything from price information to weather reports. Oracles can be bi-directional and serve to „send" data into the real world. Oracles put the data on the blockchain, meaning nodes replaying the transaction will use the same immutable data that everyone can see. To do this, an oracle typically consists of a smart contract and some off-chain components that can query APIs and then periodically send transactions to update the smart contract data.
We call it an oracle problem that certain transactions cannot directly access off-chain data. At the same time, if the system relies on a single source of truth when providing data, it is not considered a secure solution. The oracle problem can be avoided by using a decentralized oracle that collects information from multiple data sources – in this case, if one data source is hacked or its data provision fails, the smart contract will still function as intended. (see Ethereum. *Oracles*, 6 May 2022. https://ethereum.org/en/developers/docs/oracles/. [accessed: 15.09.2022]).

more customizable, flexible, and dynamic than smart contracts because they are not bound by restrictions embedded in self-executing code[34].

Among the reservations expressed against smart contracts, it should also be mentioned that general principles such as good faith, legitimate expectation, public interest, or reasonableness are mostly impossible to write in codes – i.e. the basic cornerstones of civil law have a limited ability to assert themselves in the automatic execution of smart contracts during its execution[35]. Hybrid contracts are known to deal with this problem, some of which are drawn up in a traditional format and others in a coded form. The parties must clarify with each other the exact conditions under which their legal relationship exists because the binding force of the performance obligation initiated based on the automaticity of the smart contract is equivalent to that of any other legal agreement[36].

In healthcare, smart contracts are primarily important in insurance payments and, possibly, reimbursement of the expenses for individual services. They are also used with great success by the pharmaceutical industry. The latter is justified, for example, by the fact that the drug supply chain is complex, the owners of the drugs change from the moment the formulations leave the manufacturer until they reach the customers, and without transparency, it becomes difficult to track the originality. Blockchain and smart contracts can also simplify the financial settlement of the drug from the factory to the pharmacy.

Another interesting area of application – and the understanding of the operation of smart contracts may be further facilitated by this example – is the case of so-called cold chain pharmaceuticals. Certain medicinal products must be refrigerated throughout the supply chain, from the manufacturer to the pharmacy – called the cold chain. According to the traditional solution, the cooling level can be „secured" by drivers manually checking the temperature gauge during the transport process and possibly reporting it.

[34] Joao Pedro Quintais, Balazs Bodo, Alexandra Giannopoulou, Valeria Ferrari, „Blockchain and the Law: A Critical Evaluation" *Stanford Journal of Blockchain Law & Policy*, No. 1 (2019): 91.

[35] For more on the subject, see Primavera De Filippi, Aaron Wright, *Blockchain and the Law – The Rule of Code* (Cambridge, Mass.: Harvard University Press, 2019); Alexander Duisberg, *Smart Contracts and the Law.* Presentation. Münchner Kreis – Blockchain Conference, 23 November 2017.

[36] In practice, this means that if a smart contract, for example, initiates a penalty payment from the obligee's bank account, it is not possible to revoke it on its own by referring to the fact that the breach of contract took place despite the fact that the obligee acted in accordance with the requirement of legitimate expectation.

Blockchain combined with IoT[37] promises an automatic, safer solution: Internet-connected sensors can be placed in shipping containers or trucks transporting medicines. These sensors can record the temperature regularly, even every few minutes, and send these temperature readings to a smart contract that can record them on the blockchain. The smart contract can do several things when the temperature value exceeds a certain threshold. For example, it can send an alert to the shipping company to take action to restore the temperature. If high temperatures are maintained long enough for a batch of medicine to go bad, the smart contract can withhold shipping payments to the shipping company[38].

Concerning smart contracts, an additional legal issue is whether such a legal declaration can be suspended in effect, void in content, or open to challenge. The use of suspension algorithms can be simple – of course, depending on the nature of the condition, it can be easier or more challenging to program. Nullity and changeability are more difficult issues because if the blockchain system crosses state borders, it is questionable whether national civil law regulations can be applied to it. In such cases, an important detail is the stipulation of the applicable law in the smart contract. Suppose the algorithm to be executed automatically operates under conditions that result in nullity or challengeability according to national law. In that case, the party affected by the loss of interest can act according to the regulations applicable to traditional contracts.

4. Development directions

Blockchain technology offers many opportunities for healthcare; however, many technical and organizational challenges must be faced before providers can uniformly apply healthcare blockchain.

Healthcare providers update patients' general clinical data set each time they provide care services. This information includes standard information, such as the patient's gender and date of birth, and information specific to the service, such as the procedure performed, plan of care, and other notes.

[37] IoT: The acronym stands for Internet of Things. The IoT is a system of interconnected computing devices, mechanical and digital machines, objects, animals, or people that have unique identifiers (UIDs) and are capable of transferring data over a network without the need for human-human or human-computer interaction. (Alexander S. Gillis, „What is the Internet of Things (IoT)?" *Techtarget*, March 2022. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT. [accessed:15.09.2022]).

[38] Exyte, *How Pharmaceutical Supply Chain Benefits From Smart Contracts in 2020*. https://exyte.com/blog/how-pharmaceutical-supply-chain-benefits-from-smart-contracts. [accessed: 15.09.2022].

Traditionally, this information is tracked within a single organization or in a multi-stakeholder network database[39].

The aim of the healthcare application of the blockchain would be that the flow of information shall not be interrupted at the individual or organizational level; instead, the standardized information set of each patient could be directed to the transaction layer of a national blockchain. The surface information of the transaction layer includes information not classified as protected health or personally identifiable information. Demographic data and the provided healthcare services give healthcare organizations, and research institutions access to extensive and data-rich statistical information[40].

At the same time, information stored on the blockchain can be universally accessible to an individual through its private key mechanisms, allowing patients to share their information with healthcare organizations more easily. The primary goal is, therefore, to achieve interoperability: healthcare systems[41] should operate with connected records and a common organizational architecture and standardized system. The state-level form of this solution is possible, but at the same time, the idea of a network capable of providing the same service on an international level cannot be neglected either. At the same time, I believe that due to the question of the uniformity of the legal framework, international cooperation must remain within the borders of the European Union.

4.1. Legislative proposals

Health policymakers must engage deeply with the information technology sphere to understand and facilitate systemic development within existing regulatory frameworks and emerging policy objectives. Legislative

[39] Private practice networks are examples of the latter one.

[40] Krawiec et al., *Blockchain: Opportunities,* 4.

[41] In the framework of the *organizational architecture*, the general architecture design principles can be applied for the purpose of structuring and designing IT in such a way that it fits the organizational and business strategy. Within this, the *information architecture* deals with the activities carried out by the organization and the information required for them, the *organizational information system architecture* describes the organizational information systems and the information that the systems primarily store in order to support the information architecture; the *technical and IT architecture* operates with the standards and techniques, *application architecture* deals with regulatory and policy details. See more: Ádám Tarcsi, László Sas, Bálint Molnár, Zénó Szabó, *SAP NetWeaver alkalmazásfejlesztés* (Budapest: ELTE Társadalomtudományi Kar, 2012). http://sap.elte.hu/tananyag/abap_nw/index.html. [accessed: 15.09.2022].

consideration should address the distributed data storage nature of blockchain, issues of ownership of records, and the establishment of access guarantees.

The legislator must define the conditions through which personal health data can be protected[42] while respecting the right to privacy; limits and conditions must be defined regarding the use and disclosure without patients' consent. Under certain conditions, blockchain can handle sensitive data by isolating and encrypting the customers' identities. As I explained earlier, patients can share different identity attributes with the healthcare provider system as needed and in light of their choice.

The type of detailed demographic information stored on the blockchain also requires consideration because combining this with location data theoretically enables the identification of a specific individual by triangulation. For example, identifying a person with a rare health condition may be more successful in a rural area than in a densely populated urban environment. Through a permissioned blockchain, unauthorized access can be minimized to a certain degree, but it cannot be eliminated since the permission holder usually has access to records that are not directly within his scope of supply.

I would like to add: legislative challenges do not stop purely in the sphere of law. Legal and IT professionals should cooperate closely; I think here primarily that different standards should be developed for interoperability. The ISO/TC 307 standard[43] is already suitable to bring together blockchain and distributed ledger technologies, but of course, further developments can be useful for the industry[44].

In addition to this, or perhaps even more precisely for the sake of everything, the legislator needs to support the creation of sandboxes that provide a safe framework for testing and respond actively and effectively to new

[42] In order to apply the law uniformly, describing the definition of health data is unavoidable. The GDPR applies a general definition according to which data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

[43] ISO Technical Committees, *ISO/TC 307 Blockchain and distributed ledger technologies*. https://www.iso.org/committee/6266604.html. [accessed: 15.09.2022].

[44] Additional standards related to blockchain technology, already adopted and still under development, can be found on the ISO website: https://www.iso.org/committee/6266604/x/catalogue/p/1/u/1/w/0/d/0. [accessed: 15.09.2022]. These standards related to the 307 standard are in connection with system design, usage, vocabulary, identity management, smart contracts, interoperability framework, and governance.

solution proposals after successful test operations. As far as possible, it is necessary to provide adequate support for open-source tools since, with their help, a wider circle can be involved in correcting errors, and distribution is also easier[45].

4.2. Trading health data

Providing health data with a financial value is a well-known issue in the literature, for which the system of health tokens is an effective and safe method when applying the blockchain. It is important to state that the following applies only to cases where the data is not processed in the patients' vital interest or the public interest affecting public health.

Tokens are well-known in the context of blockchain technology and cryptocurrencies. A token is a digital asset with a payment function or some other form of utilization – and in the case of so-called hybrid tokens, both. It appears from the literature that by using the blockchain, we can also „tokenize" health data, i.e., we would store the records in standardized formats, providing them with economic value and, at the same time, guaranteeing interoperability.

In recent years, several surveys have been conducted on the conditions under which respondents would hand over their health data for research purposes. In many cases, the people involved answered that they would be happy to provide the data in question in exchange for, for example, a certain reduction in social security fees. However, most of them maintain that they want to decide who can access the data[46]. It follows that health systems need to encourage individuals to exercise control over their data, but at the same time, the technical infrastructure is required where anyone seeking data can request consent for the use and, where appropriate, sharing of health data.

Blockchain technology can help create such an infrastructure as a decentralized marketplace where the individual controls access to health data. Information seekers can post their questions, and individuals can remain anonymous and decide whether or not to share their information. With the tokens on the blockchain-based marketplace, the consideration can be automatically transferred based on a digital contract after the data has been delivered.

Information seekers provide tokens to encourage individuals to digitize and share their data, while individuals can: a) redeem bonuses/services

[45] Steven Wright, *Technical and Legal Challenges for Healthcare Blockchains and Smart Contracts* (Atlanta: Előadás. ITU Kaleidoscope, 2019).

[46] Eberhard Scheuer, „ Blockchain Solves Healthcare Data Obstacles" *HealthManagement*, No. 1 (2019). https://healthmanagement.org/c/hospital/issuearticle/blockchain-solves-healthcare-data-obstacles. [accessed: 15.09.2022].

offered by providers on the platform; b) they can exchange it for another cryptocurrency; or c) can be exchanged for cash at designated currency exchanges. Individuals can monetize their data stored in external databases and share it with the owners of the information, such as personal health records, claims handlers, hospitals, or even pharmacies. The tokens' value depends on how much the network participant values the information[47].

Suppose we accept the endowment of health data with material value in this form. In that case, it can only be achieved with blockchain technology since the transaction processes are transparent and, at the same time, more efficient. A blockchain-based token system can align incentives between ecosystem participants, such as health information providers and those seeking to analyze health data. It allows the latter to directly access providers of health information without the use of intermediaries. At the same time, it will enable individuals to control the use and monetization of their health data. The tokenization of health data incentivizes individuals to make their data sharable, solving a fundamental problem in modern healthcare[48].

Bibliography

Agnikhotram Sai, Antonios Kouroutakis, „Doctrinal Challenges for the Legality of Smart Contracts: Lex Cryptographia or a New, Smart Way to Contract” *Journal of High Technology Law*, No. 2 (2019): 300-328.

Árpási Zoltán, „A blokklánc alkalmazásának lehetőségei az egészségügyben” *Cryptofalka*, 29 December 2019. https://cryptofalka.hu/blokklanc-egeszsegugyi-alkalmazasa/.

Becker Katrin, „Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries” *Law and Critique*, 33 (2022): 113-130. https://link.springer.com/article/10.1007/s10978-021-09317-8.

Bennett Kathryn M., „HealthTech: How Blockchain Can Simplify Healthcare Compliance” *Washington and Lee Journal of Civil Rights and Social Justice*, No. 1 (2018): 287-314.

Berson Dave, Susan Berson, „Blockchain Law 101: Understanding Blockchain Technology and the Applicable Law” *Journal of the Kansas Bar Association*, No. 2. (2019): 40-43.

Brewer Clay, „Help Us, Help You: Big Tech and the Future of Personal Health Records” *Belmont Health Law Journal*, 3 (2019): 74-116.

Chang Josephine, Alek Emery, „Blockchain Patentability 101” *Los Angeles Lawyer*, No. 6 (2019): 20-25.

[47] Scheuer, „Blockchain Solves”.

[48] Ibidem.

CNIL, *Solutions for a Responsible use of the Blockchain in the Context of Personal Data*. September 2018; https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

Connor-Green Devon S., „Blockchain in Healthcare Data" *Intellectual Property and Technology Law Journal*, No. 2 (2017): 93-108.

De Caria Riccardo, „Blockchain and Smart Contracts: Legal Issues and Regulatory Responses between Public and Private Economic Law" *Italian Law Journal*, No. 1 (2020): 363-379.

De Filippi Primavera, Aaron Wright. *Blockchain and the Law – The Rule of Code*. Cambridge, Mass.: Harvard University Press, 2019.

DHL: *DHL and Accenture Unlock the Power of Blockchain in Logistics*. Bonn, Germany, 03/12/2018; https://www.dhl.com/global-en/home/press/press-archive/2018/dhl-and-accenture-unlock-the-power-of-blockchain-in-logistics.html.

Dimitropoulos Georgios, „The Law of Blockchain" *Washington Law Review*, No. 3 (2020): 1117-1192.

Duisberg Alexander, *Smart Contracts and the Law*. Presentation. Münchner Kreis – Blockchain Conference, 23 November 2017. https://www.muenchner-kreis.de/wp-content/uploads/fileadmin/dokumente/_pdf/20171123/Duisberg_20171123_MKreis_Blockchain_Dr._Alexander_Duisberg_final.PDF.

Ethereum, *Oracles*, 6 May 2022. https://ethereum.org/en/developers/docs/oracles/.

Exyte, *How Pharmaceutical Supply Chain Benefits From Smart Contracts in 2020*. https://exyte.com/blog/how-pharmaceutical-supply-chain-benefits-from-smart-contracts.

Finck Michèle, „Blockchains and Data Protection in the European Union" *European Data Protection Law Review*, No. 1 (2018): 17-35. https://edpl.lexxion.eu/article/edpl/2018/1/6/display/html.

Gillis Alexander S., „What is the Internet of Things (IoT)?" *Techtarget*, March 2022. https://www.techtarget.com/iotagenda/definition/Internet-of--Things-IoT.

Interpol, *Fake Medicines*. https://www.interpol.int/Crimes/Illicit-goods/Shop-safely/Fake-medicines.

Johnson Walter G., „Blockchain Meets Genomics: Governance Considerations for Promoting Food Safety and Public Health" *Journal of Food Law and Policy*, No. 1 (2019): 74-97.

Krawiec R.J., Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai. *Blockchain: Opportunities for Health Care*. Deloitte, August 2016. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf.

Leck Andy, Ren Jun Lim, „A Peek into the Health Tech Boom” *Managing Intellectual Property*, 251 (2015): 33-35.

Lingwall Jeff, Ramya Mogallapu, „Should Code Be Law? Smart Contracts, Blockchain, and Boilerplate” *UMKC Law Review*, No. 2 (2019): 285-322.

Mi az a blokklánc? Átfogó útmutató és *jövőbeli alkalmazási területei*. https://www.bitcoinbazis.hu/utmutato/blokklanc-utmutato/.

Móray Gábor, „Mi az a blokklánc technológia és milyen lehetőségeket kínál?” *Computerworld*, 28 Octtober 2020. https://computerworld.hu/tech/mi-az-a-blokklanc-technologia-es-milyen-lehetosegeket-kinal-285890.html.

Nadimi Peter, Samuel G. Korver, Zach Smolinski, Lauren M. W. Steinhaeuser, Corey Bieber, „Practicing Blockchain Law [comments] Panel III” *John Marshall Journal of Information Technology and Privacy Law*, No. 1 (2019): 52-73.

OECD, „Opportunities and Challenges of Blockchain Technologies in Health Care” *Blockchain Policy Series* (December 2020).

Quintais Joao Pedro, Balazs Bodo, Alexandra Giannopoulou, Valeria Ferrari, „Blockchain and the Law: A Critical Evaluation” *Stanford Journal of Blockchain Law &* Policy, No. 1 (2019): 86-112.

Pena Daniel, „Blockchain and Data Protection: Health Patients Records in Colombia” *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, No. 6 (2019): 29-31.

Rauland Marco, *Are You Smart Enough? Blockchain & Smart Contract Applications in Pharma.* 10.02.2022; https://pharmaboardroom.com/articles/are-you-smart-enough-blockchain-smart-contract-applications-in-pharma/.

Rejeb Abderahman, Horst Treiblmaie, Karim Rejeb, Suhaiza Zailani, „Blockchain Research in Healthcare: A Bibliometric Review and Current Research Trends” *Journal of Data, Information, and Management*, 3 (2021): 109-124. https://doi.org/10.1007/s42488-021-00046-2.

Saunderson Doreen, Margaret Mrazek, „High Tech Medical Advances and the Health Law Labyrinth” *Law Now*, No. 6 (1990): 8-11.

Scheuer Eberhard, „Blockchain Solves Healthcare Data Obstacles” *Health Management*, No. 1 (2019). https://healthmanagement.org/c/hospital/issuearticle/blockchain-solves-healthcare-data-obstacles.

Schrepel Thibault, *Anarchy,* „State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia” *Social Science Research Network*, 12 November 2019. https://ssrn.com/abstract=3485436.

Stines Robert A., „Blockchain 101: A Lawyer's (Brief) Guide” *Tort Source* (2019): 14-15.

Tarcsi Ádám, László Sas, Bálint Molnár, Zénó Szabó, *SAP NetWeaver alkalmazásfejlesztés.* Budapest*:* ELTE Társadalomtudományi Kar, 2012.

Van Eecke Patrick, Anne-Gabrielle Haie, „Blockchain and the GDPR: The EU Blockchain Observatory Report” *European Data Protection Law Review (EDPL)*, No. 4 (2018): 531-534.

Werbach Kevin, „Trust, but Verify: Why the Blockchain Needs the Law” *Berkeley Technology Law Journal*, No. 2 (2018): 487-550.

Wright Aaron, Primavera De Filippi. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia Social Science Research Network*, 10 March 2015. http://dx.doi.org/10.2139/ssrn.2580664.

Wright Steven, *Technical and Legal Challenges for Healthcare Blockchains and Smart Contracts.* Atlanta: Presentation. ITU Kaleidoscope, 2019.

Yeung Karen, „Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code of Law and Code as Law” *Modern Law Review*, No. 2 (2019): 207-239.