The current stage of IT development has considerable potential to address the challenges of improving the quality of healthcare services. At the same time, the use of digital technology poses serious challenges for governments to improve the quality of healthcare and pharmaceuticals. Today when digital technologies become more important, it is no longer possible to imagine our life without blockchain, a fault-tolerant decentralized system, the core principles of which are that each subsequent block in the blockchain contains the hash value of the previous block, and all attempts to change the data recorded on a particular block levels, will cause changes at all subsequent levels and will be noticed by other participants (network nodes). This ensures database integrity verification and a blockchain sequence is formed in which each subsequent block stores the hash value of the previous one [2, 277].

Blockchain has gone far beyond cryptocurrencies, and has spread to all walks of life in society and the state, and thanks to its coordination capabilities and the ability to retain information has become a modern Magna Carta of fundamental social progress. The advantage of blockchain over other storage media is that the data that gets to it can be analyzed while remaining private and unchanged [3, 149-150].

Theoretical, blockchain can be applied to any database and provide reliable storage of information. Blockchain technology has the potential to transform healthcare, placing the patient at the center of the health care ecosystem and increasing the security, privacy, and interoperability of health data. This technology could provide a new model for health information exchanges (HIE) by making electronic medical records more efficient, disintermediated, and secure [4].

The technical features of blockchain have been the subject of many research works [2; 4; 5], at the same time, the legal aspects of this technology were fragmented, and were mainly devoted to the legal regulation of blockchain usage in the context of fintech industry in different countries of the world [6; 7; 8].

The question of protecting human rights on privacy, including the right to personal information, non-disclosure of medical information, and human rights to quality medicines, remain relevant today. At the same time, it should be noted the complete absence of theoretical elaboration of the problems of legal regulation of relations with the use of blockchain technology in this field.

Tracking drug chains, storing patient records, health insurance are the part of incomplete list of options to use distributed database technology in healthcare. The research of legal issues arising from the use of blockchain technology in the field of human rights is fragmented.

**THE AIM**

The aim of the study is to examine the blockchain technology in the field of healthcare, to analyze the principles of the European Convention on Human Rights regarding...
respect for private and family life, home and correspondence, to analyze the key positions of the European Court of Human Rights (hereinafter – ECHR) in the field of human rights to privacy, to analyze the European Union (hereinafter – EU) secondary legislation regarding the supply of medicines, prospects for the blockchain usage in order to protect human rights to privacy and improve the quality of medicines.

MATERIALS AND METHODS
Scientific works that are devoted to the dissemination of digital technologies in healthcare, the provisions of the European Convention on Human Rights, the ECHR’s practice on the protection of human rights on privacy, the provisions of the EU secondary legislation regulating the supply of medicines are studied. The methodology of this article is built upon comparative and legal analysis techniques and includes system-structural method, method of generalization, method of analysis and synthesis as well.

REVIEW AND DISCUSSION
As it mentioned in Deloitte’s 2019 Global Blockchain Survey, 40 percent of health professionals see blockchain as a top priority. In addition, the global healthcare market is expected to spend $ 5.61 billion by 2025, according to a report by BIS Research «Global Blockchain in Healthcare Market- Analysis and Forecast, 2017-2025». The adoption of the blockchain technology will help save the industry up to $ 100-150 billion per year by 2025 in data breach-related costs, IT costs, operations costs, maintenance and staffing costs, and through a reduction in frauds and counterfeit products [9].

The first launch of blockchain took place in 2009 and was only associated with cryptocurrency, but since 2014 other blockchain opportunities have been discussed greatly. In particular, the attention to the potential of a decentralized approach and the use of such a consensus mechanism whereby the final state of database accounting system would be well protected against change was drawn. Blockchain, as a way of organizing data storage, has enabled accounting systems with multiple independent validators to achieve not only secure synchronization of databases, but also the invariability of this data, subject to some assumptions [2, 274].

The formidable innovation introduced by blockchain is that the network is open and participants do not need to know or trust each other to interact: the electronic transactions can be automatically verified and recorded by the nodes of the network through cryptographic algorithms, without human or any other intervention (banks, financial institutions or other organizations). Blockchain has become “a disruptive innovation with a wide range of applications, potentially able to redesign our interactions in business, politics and society at large” [10, 45].

In healthcare, the issue of information management is very topical. Healthcare providers work daily with data that requires careful handling, anonymity, and correct transfer of information. It also requires specific rules regarding access to medical data, a specific algorithm for managing rights, developing common standards for entering and handling “big data”.

The protection of personal data, including medical information, is a fundamental feature of the right to privacy [11]. Medical data are subject to both Article 8 (1) of EU Directive 95/46 / EC on data protection [12] and Article 6 of Council of Europe Convention No 108 [13], which stipulate in particular that personal data concerning health, may not be processed automatically unless domestic law provides appropriate safeguards.

To protect personal information stored in automated databases, appropriate security measures for preventing their accidental or unauthorized destruction or accidental loss, as well as preventing their unauthorized access, alteration or distribution of such data should be taken.

In the thematic report “Health-related issues in the case-law of the European Court of Human Rights” the Court has acknowledged that the protection of personal data, including medical information, is of fundamental importance to the enjoyment of the right to respect for his or her private and family life guaranteed by Article 8 of the Convention [14].

In I. v. Finland the applicant, an HIV-positive nurse, suspected that unauthorised persons had accessed her medical records. While the strict application of domestic law would have constituted a substantial safeguard in her case, the system at the hospital made it impossible to clarify retroactively the use of patient records or to determine whether information contained on the applicant and her family had been given to or accessed by unauthorised parties. Moreover, at the material time the records could also be read by staff not directly involved in her treatment. Although the hospital had subsequently taken ad hoc measures to protect the applicant against unauthorised disclosures by restricting access to treating personnel and registering her under a false name and social-security number, this had come too late. What had been required in the applicant’s situation was practical and effective protection to exclude any possibility of unauthorised access occurring in the first place. The Court therefore found a violation of Article 8 [15].

According to the requirements of Article 8 of the Convention, the use of samples of human biological materials (cell samples, DNA data, fingerprints) in criminal proceedings should also be mentioned.

Rules for the use and storage of biological samples of human tissues (including DNA data) in the investigation of crimes are set out in Council of Europe Committee of Ministers Recommendation No. R (92) 1 of 10 February 1992 “On the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system” [16]. However, in spite of the high level of regulation of the problem, there is the concern in society about human rights abuses during the creation and use of DNA databases [17, 151].
Currently, there is no standard in Ukraine for the storage and transmission of medical data. In June 2019, the Ministry of Health of Ukraine proposed a draft decree of the Cabinet of Ministers of Ukraine “On approval of the Health Informatization Concept of Ukraine” [18]. The concept presented contains a strategic plan for the development of the e-Health system, basic principles of its operation, necessary legislative changes and prerequisites for the investment attractiveness of the system.

It is envisaged to solve the problem of inadequate level of efficiency and transparency of health care, which leads to inefficient use of resources, by ensuring timely and reliable information for the state institutions involved in the management of the health care system, by using the benefits of handling «Big Data” and intelligent systems to predict health care needs, by planning resources in the industry and engaging the patient in their own health care, by monitoring the quality of the medical services received by providing access to and disposal of their own medical data.

Data fragmentation will be avoided due to the electronic system which will allow to store patients’ data in a secure cloud storage facility instead of paperwork and which will allow doctors of different medical institutions to have access to the necessary information.

It is stated in the analytical note to the Cabinet of Ministers of Ukraine as for the project, the process of electronic health system introduction in Ukraine is characterized by lack of compatibility of information systems in the field of health care, lack of a unique identifier for patients, imperfection of information infrastructure and interaction between general registers, imperfection of a number of registers, absence of specialist staff for automation and change management, lack of computer and networking equipment in healthcare facilities, etc. [19].

Within 2017–2018, a number of systematic changes in the field of health informatization took place, a number of by-laws regulating the activity of the electronic health care system and institutions were implemented – Ministry of Health, National Health Service of Ukraine, State Enterprise “Electronic Health”.

E-government is being introduced in Ukraine as a modern tool of the effective interaction between the state, civil society and business, which is intended to fully implement the rights and interests stipulated by the legislation, to use effective mechanisms of rights and freedom protection, to influence the actions or inactivity of state authorities and to hold their officials responsible in cases established by law [20, 52] and the possibility of access to the system of interaction of state electronic resources “Trembita” is being expected. Activities in this field are conducted by the State Agency for Electronic Governance of Ukraine.

Undoubtedly, it is difficult to overestimate the importance of the proposed concept for the future of e-health and medical reform. At the same time, its imperfection should be mentioned. One of the vulnerabilities of the medical field, and the concept, unfortunately, does not provide a solution to this problem, is the protection of patients’ personal data and the issue of responsibility for their accessibility and preservation. It is also unclear what the concept of security is, what the means of patient authentication are.

According to the Article 3 of the European Charter of Patients’ Rights, every person has the right to receive full information on health status, medical care, including medical interventions, the possibilities and conditions of use of the results of medical care and all available modern technologies [21].

Blockchain technology opens up very interesting and promising storage, transmission and data management capabilities. Among the blockchain projects which have been already implemented the following ones can be pointed out. Iryo is a platform for storing and controlling patients’ electronic medical records based on blockchain EOS. CareX is a project that develops through healthcare payments through its CareX token. Increased demand for medical tourism requires cross-border transfers or the use of large amounts of cash. The project solves this problem by using CareX’s internal cryptocurrency. Token owners can store their medical information in the system, completely controlling their privacy and making them available as needed. The platform provides support for a chatbot with artificial intelligence that can make previous diagnoses.

SmartHealthCareToday is a platform for storing personal medical data, integrating EHR (Electronic Medical Card) and PHR (Personal Medical Card) with information about a patient’s life, activity, and regular measurements of medical parameters such as blood pressure and blood glucose. Access to health data through in-app users can be tailored to each patient by the program. Brdrt.pro lab has conducted research of blockchain projects focused on health care work and has counted over 20 medical data storage and management solutions. Today it is the most popular field of development in medicine [22].

According to WHO information, one in ten medicines distributed in low- and middle-income countries is either non-conventional or counterfeit [23]. The current model of state regulation of the medicines supply in Ukraine does not provide medicines of the proper quality, which does not only cure but can also cause serious illness or even patients death.

As the rules of the EU’s “secondary law” acts are not the acts of direct effect in Ukraine, their implementation is necessary therefore. To address this issue, national legislation should be harmonized with EU law in accordance with the EU-Ukraine Association Agreement and its annexes.

The implementation of the requirements of the above mentioned documents of the European Union is intended to facilitate the regulation of legal relations in the sphere of circulation of medicines related to the creation, issuance of trade licenses, production, import, wholesale and remote trade, quality control of medicinal products, definition of these rights and obligations, as well as the powers of public authorities in this area.

As defined in point 33 of Section I of Directive 2001/83 / EC, a falsified medicinal product is any medicinal product with a false representation of:
(a) its identity, including its packaging and labelling, its name or its composition as regards any of the ingredients including excipients and the strength of those ingredients;
(b) its source, including its manufacturer, its country of manufacturing, its country of origin or its marketing authorisation holder; or
(c) its history, including the records and documents relating to the distribution channels used [24].

Global trends in medicines counterfeiting counteraction combine effective mechanisms for combating the spread of counterfeit medical devices at international, European regional and national levels [30].

The effectiveness of the drug control mechanism and the liability of individuals for drug law offenses can be significantly improved by the use of blockchain technology, which can be a solution to improve data security, integrity, functionality and, of course, the security of the pharmaceutical supply chain. This technology can be used to overcome the problem of identity identification, sources of origin, as well as the history of drug distribution, as it will allow tracing the entire supply chain, preventing falsification as such [31].

Thus, blockchain is a real revolution in the healthcare industry as it is well suited to protect all aspects of distributed networks and helps to record, store, sort and transmit data in such a way that they remain relevant and unchanged. Once the supply chain (medicines) becomes visible and transparent with the help of blockchain, it will be possible to trace the origin of the medicines (the quality of the medical services provided). Beneficiaries of blockchain technology will be healthcare facilities and pharmaceutical companies by reducing the costs of counterfeit products and patients receiving quality medicines.

The use of blockchain technology not only minimizes the risks of supplying counterfeit medicines to patients, but also ensures transparency of delivery and reduction in price of the final product for patients [32].

Blockchain issues have been developed in the works of Swan Melanie [3], Arvind Narayan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder [5], Atzori M. [10], who have focused on blockchain as the latest digital technology capable cause profound changes in society and are, to some extent, debatable. In particular, blockchain and decentralized platforms are explored as hyperpolitical tools capable of managing large-scale social interactions and abolishing the traditional vertical of power as such. The analysis highlights the risks associated with the dominance of private interests in distributed ecosystems, which could lead to the emergence of a global, stateless society.

The introduction of blockchain technology was investigated in the work of V. Pashkov, which emphasized the need for adequate legal support for the full involvement of this technology in the field of pharmacy [32].

The vulnerability of human rights to the formation of DNA databases is one of the objects of study by M. Goc, H. Dłbrowska [17]. In turn, the relationship between the privacy of information contained in human DNA and the public interest in using such information in the investigation of crimes is a subject of debate in R. Erbaş’s work [33].

CONCLUSIONS

Global health trends aim to improve the protection of human rights to respect for privacy and the quality of medicines. The analysis of EU legislation shows that the protection of human rights for quality healthcare is provided at the conventional level, on the basis of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as at the level of secondary law acts, with further implementation in the national legislation of the states.

Health informatization allows us to see the prospects of blockchain using to protect human rights in the fields of medicine and pharmacology. Overcoming the problems of storing and managing patient data, tracking the origin of medicines, maintaining data consistency while designing medicines are just some of the challenges that blockchain has successfully handled.

The use of artificial intelligence, big data analytics and blockchain can work together to ensure efficiency and accurate results in the medical and pharmaceutical environment, and thus increase the level of human rights protection for quality healthcare. Further research are in need to assess the possible risks and costs associated with blockchain, and to take into account the legal aspects of technology implementation and to bring them into line with current legislation of countries.

REFERENCES


1542


23. 1 in 10 medical products in developing countries is substandard or falsified. https://www.who.int/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified


**ORCID and contributions:**
Volodymyr V. Marchenko: 0000-0003-1921-3041 A,B,D,E,F
Inna L. Kilimnik: 0000-0003-3225-6257 A,B,D,E,F
Alla V. Dombrovskaya: 0000-0003-4610-8220 A,B,D,E,F
Conflict of interest:
The Authors declare no conflict of interest

CORRESPONDING AUTHOR
Alla V. Dombrovska
O.M. Beketov National University of Urban Economy in Kharkiv
17 Marshala Bazhanova st., 61000 Kharkiv, Ukraine
tel: +380503027714
e-mail: dombrovskalla@gmail.com

Received: 21.01.2020
Accepted: 17.06.2020

A – Work concept and design, B – Data collection and analysis, C – Responsibility for statistical analysis,
D – Writing the article, E – Critical review, F – Final approval of the article