International Law Review, Volume 42, Issue 78, Summer 2025/ pp. 157-177

Effective Factors in Solving the Legal Gaps of Blockchain-based Systems in Dealing with Counterfeiting of Drugs
(Original Research)

Afsaneh Ghanbari *
Amir Mahmoudi **
Behnam Habibi Dargah ***

(DOI): 10.22066/cilamag.2024.2029532.2561
Date Received: 18 May.2024 Date Accepted: 4 Nov.2024

Abstract
Drug counterfeiting causes global health corruption and hinders the achievement of the Millennium Development Goals and the right to the highest attainable level of standards of health, under Article 12 of the International Covenant on Economic, Social and Cultural Rights. In General Comment No. 14 of the Covenant, access to essential medicines is described as a human right. Although blockchain technology provides a safe and transparent method to track drugs along the supply chain to prevent counterfeiting, the results indicate that this technology has some ambiguities in terms of structure and functionality regarding compliance with existing legal regulations, namely, limitations regarding its implementation. A question can be raised in this matter, and that is, what are the effective factors in solving the existing legal gaps in relation to the laws of the digital space and blockchain? It seems that the governance of the blockchain in the decision-making process and regulation of laws are effective in how the blockchain network works.

Keywords
Legal Gaps, Blockchain, Technology, Drug, Counterfeiting

* PhD Student of International Law, Department of International Law, Karaj Branch, Islamic Azad University, Karaj, Iran; dr.ghanbari@sbmu.ac.ir

** Corresponding Author, Assistant Professor, Department of International Law, Karaj Branch, Islamic Azad University, Karaj, Iran; Amir.mahmoodi@kiau.ac.ir

*** Assistant Professor, Department of Private Law, Karaj Branch, Islamic Azad University, Karaj, Iran; drhabibi1361@yahoo.com

Introduction

The quality of medicines has been a concern of the World Health Organization ["WHO"] since its establishment in 1946.[1] According to the report of the WHO and the International Anti-Counterfeiting Coalition, drug counterfeiting has become one of the significant crimes in the world, with an estimated annual value of more than USD 600 billion.[2] WHO defines counterfeit medicine as "A medicine that is produced fraudulently is of poor quality and has an inappropriate label, the information of its source or identity is hidden and does not meet certain standards, this medicine is considered counterfeit".[3] Despite the consensus on the WHO's definition of counterfeit medicine, the definitions used in practice, or under the laws of different countries are different and create problems in data collection and implementation of countermeasures against counterfeit medicines.[4] According to the WHO definition, the drug supply chain includes various stages such as supplying raw materials, manufacturing, packaging, transportation, storage and distribution to medical centers or pharmacies. It is a complex network involving multiple stakeholders, including drug manufacturers, wholesalers, distributors, and healthcare providers, all working together to ensure that safe and effective drugs reach the people who need them. The supply chain ensures quality, safety, and availability of essential drugs worldwide.[5]

In the absence of a proper traceability mechanism, weak links arise in the supply chain, allowing drugs to be counterfeited, or counterfeit drugs to be introduced; therefore, the adoption of new technologies to establish more effective traceability mechanisms becomes essential.[6] Currently, the supply chain management system in the pharmaceutical industry does not create transparency and supervision for drug manufacturers and regulators, and is unable to resist cyber security threats (in the virtual space)[7]. Therefore, to prevent the production and distribution of counterfeit drugs, the pharmaceutical industry needs an effective supply chain management system. The solution

1. World Health Organization. *International Health Regulations* (2005). World Health Organization, 2008.

2. Muhammad Maaz, and Tahir Ali, "How Counterfeits Goods Are Destroying Brand Reputation", *Journal of Engineering and Economic Development* 6, no. 2 (2020): 38-49:39.

3. Jen-Hung Tseng, Yen-Chih Liao, Bin Chong, and Shih-Wei Liao, "Governance on the Drug Supply Chain Via Gcoin Blockchain", *International Journal of Environmental Research and Public Health* 15, no. 6 (2018): 1055.1-8:2.

4. Christopher J. Sirrs, "Fluid Fakes, Contested Counterfeits: The World Health Organization's Engagement with Fake Drugs, 1948–2017." *Medicine Anthropology Theory 10*, no. 3 (2023): 1-29:17.

5. Sujatha Alla, Leili Soltanisehat, Unal Tatar, and Omer Keskin, "Blockchain Technology in Electronic Healthcare Systems", In IIE Annual Conference. Proceedings, pp. 901-906. *Institute of Industrial and Systems Engineers* (IISE), (2018): 2.

6. Dingyuan Zhang, and Caiqian Cheng. "AI-Enabled Product Authentication and Traceability in Global Supply Chains." *Journal of Advanced Computing Systems* 3.6 (2023): 12-26:13.

7. Hasan, Khondker Shajadul, and Shezad Rouf Khondker. "Utilizing Blockchain Technology in Cyber Security to Secure Pharmaceutical Industry Supply Chain." *Conference Paper*. (2022):1.

that can be offered to develop a suitable system is the blockchain technology.[8] It is assumed that blockchain technology can provide reliable and transparent tracking of data stored in the drug supply chain due to its technical features such as decentralization, uniqueness of data, determination of transaction records, etc. The question is, what are the legal issues of using blockchain technology in the pharmaceutical industry? Further, how will the regulation of access to this technology prevent falsification of transaction records? Will the existing laws adequately cover the issues related to the mentioned topics in this technology, such as determining jurisdiction, governing law, intellectual property protection and information privacy? Without clear and coherent laws in this field, which approach and performance is applicable for the effectiveness of measures to prevent drug counterfeiting?

In 2019, Lishfield concluded in an article titled "A Review of Healthcare Information Management Systems Problems and Blockchain Solutions" that blockchain,[9] a chain of blocks, manages the supply chain through data record checking, tracking, and authentication.[10] However, the above article does not mention possible legal challenges to data falsification in the supply chain based on blockchain technology.

Due to the urgency of the vital issue of medicines and their influential role in the society's wellbeing, this article focuses on the existing laws and regulations surrounding blockchain technology and examines how the current legal frameworks may include gaps that allow illegal activities to occur within the blockchain; Activities such as money laundering, fraud, and forgery in drug supply chains.

The authors present a proposal to address the existing gaps. This research is grounded in an analytical-descriptive method, relying on reputable library documents and sources. The theoretical framework of the research is justice-based rights, drawing from Rawls' theory of justice. It underscores the significance of fairness and equal access to resources and opportunities for all individuals. Hence, the prohibition of drug counterfeiting is imperative to ensure universal access to safe and effective drugs, promoting justice and safeguarding public health.

In this article, we first briefly explain the pharmaceutical industry's anti-counterfeiting technologies, and then examine the legal issues related to implementing blockchain technology under the existing international documents in the law applicable to cyberspace. Ultimately, we provide a solution to blockchain technology's legal problems.

8. Peng Zhu, Jian Hu, Yue Zhang, and Xiaotong Li, "A Blockchain Based Solution for Medication Anti-Counterfeiting and Traceability", *Ieee Access 8* (2020): 184256-184272:184260.

9. Blockchain is a distributed ledger system that contains a sequence of blocks or units of digital information that are sequentially stored in a public database.

10. A. Litchfield, and Arshad Khan, "A Review of Issues in Healthcare Information Management Systems and Blockchain Solutions", (2019):4.

1. Identifying the Causes of the Spread of Counterfeit Drugs

The WHO, a reputable authority, has meticulously identified numerous factors that contribute to the proliferation of counterfeit drugs.[11] These factors include inadequate regulation of national drug production and distribution, lax enforcement of existing laws, lenient criminal penalties for drug-related offenses, loose regulations in exporting countries' free trade zones, complex transactions involving multiple intermediaries, high demand and inflated prices of therapeutic, preventive, and vaccine drugs, and ineffective collaboration among stakeholders.

Given the above, the lack of sufficient supervision control, inefficiency or weak regulatory institutions can contribute to the import, production and distribution of illegal drugs and lead to the spread of counterfeit drugs in drug distribution channels and the emergence of illegal markets and the promotion and sale of more fake drugs. The WHO focuses more on national laws; It has yet to formulate binding international regulations and integrating national regulations, especially in drug production and distribution.

Have other international documents been compiled in this field? As follows, we will review the international documents related to drug counterfeiting.

2. Analysis of International Documents Related to Drug Counterfeiting

The extent of the problem of counterfeit drugs has forced the international community to take measures that have led to the adoption of international legal documents on their production and supply, as well as the implementation of some programs and projects.

The right to health is one of the fundamental human rights mentioned in the Universal Declaration of Human Rights and in Article 12, paragraph 1 of the International Covenant on Economic, Social and Cultural Rights.[12] Also, the necessity of this right has been mentioned in five binding legal treaties, such as the Convention on the Elimination of All Forms of Discrimination against Women, the Convention on the Rights of the Child, the International Convention on the Elimination of All Forms of Racial Discrimination, the International Convention on the Protection of the Rights of All Migrant Workers and Their Family Members and the Convention on the Rights of Persons with Disabilities.[13]

---

11. Sujatha Alla, Leili Soltanisehat, Unal Tatar, and Omer Keskin, "Blockchain Technology in Electronic Healthcare Systems", *IIE Annual Conference*. Proceedings, pp. 901-906. Institute of Industrial and Systems Engineers (IISE), (2018): 328.

12. Alice Bryk Silveira, "Risk-Creating Industries' Obligation to the Right to Health." *In Business and Human Rights*, pp. 242-264. Brill Nijhoff, (2025):242-264:244.

13. Mohammad Ali Ghanbari, Afsaneh Ghanbari, Korosh Delpasand, "The Inclusion of Traditional and Complementary Medicine in the Strategy of the United Nations and the World Health Organization", *Journal of Medical History*, 11(41), (2018). 7-22:3-6.

The Committee on Economic, Social and Cultural Rights has also described access to essential medicines as a human right in its general comment No. 14.[14] According to this interpretation, governments must ensure equal access to health care and treatment services through legislative measures, such as high-quality, healthy medicine and other health and medical goods and services.[15]

In addition, the (former) United Nations Human Rights Commission has also pointed out that access to medicine in the case of widespread diseases is a vital element for the gradual and complete realization of the right to benefit from the highest attainable level of health. Therefore, access to safe, effective and affordable pharmaceutical products is necessary to realize this right.[16]

In this context, international documents establish a robust framework for countries to fulfill their obligations to protect, respect, and implement the right to health in relation to medicinal products.[17] These documents set forth standards, guidelines, and principles that facilitate access to essential drugs, ensure quality and safety standards, and regulate the production and distribution of pharmaceutical products. They also address organized criminal activities such as drug counterfeiting, as exemplified by the United Nations Convention against Transnational Organized Crime, or agreements that tackle various issues in the field of counterfeiting, protection of intellectual and industrial property and trademarks, such as the Medicrime Convention, the TRIPS Agreement, the Paris Convention, the Madrid Agreement, the Convention of the World Intellectual Property Organization, Patent Cooperation Agreement, Intellectual Property Copyright Treaty, Convention of Rome, and Agreement on Performances and Voices of Intellectual Property.

Several key international organizations, such as the WHO, the United Nations Office on Drugs and Crime, Interpol, Europol, and the World Customs Organization, have attempted to address the global issue of counterfeit drugs. Most importantly, since 1988, the WHO has repeatedly issued resolutions and guidelines. The International Working Group on Anti-Counterfeiting of Medical Products was established in 2006 by the WHO. It included partnerships with all major organizations involved in preventing the counterfeiting of medicines and medical products. Its main objectives are to

14. Hans V Hogerzeil, "Essential Medicines and Human Rights: What Can They Learn From Each Other?." *Bulletin of the World Health Organization* 84 (2006):371-375:373.

15. CESCR, General Comment No. 14, para. 35. Committee on Economic, Social & Cultural Rights (CESCR), "The Right to the Highest Attainable Standard of Health", (article 12 of the ICESR), *General Comment, No.14. (2000)*.

16. Saber Niavarani, Ehsan Javed, "The Right of Access to Essential Medicines in the Framework of the TRIPS Agreement and the Challenge of Protecting the International Human Right to Health", *International Legal Journal*. 33 (54) (Spring-Summer) (2015), 29-58: 31.

17. Pejman Mirkarimi, Seyyed Baqer Mir Abbasi, Maryam Moradi, "Investigating the Role and Position of Intellectual Property Rights in the General International Law System" *Iranian Political Sociology Monthly*. 5(11), (2020).3368-3384:3380.

prevent the production and marketing of counterfeit drugs and enable all partners to communicate and cooperate with each other so that they can manage regulatory measures to eliminate the crime of fraud.[18]

In the meantime, there is no internationally binding document regarding the counterfeiting of drug products and similar crimes. There is also no binding international document that has criminalized the intent, planning, and certain criminal acts of drug counterfeiting.

3. Blockchain, a New Anti-Dounterfeit Technology

Counterfeit medicines are increasing in most countries. Various technological approaches are available, or have been under development, ranging from simple to complex.[19] Validation tools for counterfeit drugs, such as holograms or colour-changing inks, are inexpensive but easily copied. Invisible tools, such as invisible printing and digital signage, are more expensive and require special inspection equipment. [20] Although chemical or biological labels built into pharmaceutical packaging are safer against copying, they are more expensive and offer no significant assurance to customers. Serialization or traceability systems, using technologies such as barcodes and radio frequency identification, help to validate the drug by giving it reliability as it is tracked through the supply chain.[21] However, these technologies require more expensive technical infrastructure and are only partially immune to virtual attacks.

One anti-counterfeit technology is the fake-product detection system based on artificial intelligence. Machine learning uses the given data set to generate a conclusion as to whether the product is genuine or not. [22]

Another emerging technology is blockchain; recognized as an excellent tool for identifying counterfeit products and removing them from the supply chain or retail market. It allows users to check and identify the product information they want quickly. [23] Blockchain is a decentralized, distributed ledger that contains records of transactions and maintains them in a peer-to-peer network. Each data must be placed at the end of a chain according to a predetermined pattern to prevent distortion or falsification. In addition to its

18. Gopakumar, K. M., and Sangeeta Shashikant. *Unpacking the Issue of Counterfeit Medicines*. Penang, Malaysia: Third World Network, (2010):22.

19. Ishaan Singhal, Himanshu Singh Bisht, and Yogesh Sharma, "Anti-Counterfeit Product System Using Blockchain Technology." *Int. J. Res. Appl. Sci. Eng. Technol* 9.12 (2021): 291-295:292.

20. Ranjana Pathak, *et al.* "Tackling Counterfeit Drugs: the Challenges and Possibilities." *Pharmaceutical Medicine* 37.4 (2023): 281-290: 286.

21. Mahmoud Farouk El Feky, "Using New Digital Anti-Counterfeiting Technologies to Protect the Egyptian Pharmaceuticals Packages Against Counterfeiting." *International Design Journal* 10.3 (2020): 187-192:188.

22. *ibid* n.20.

23. Renata Hrecska-Kovacs, "Health Law Implications of the Use of Blockchain Technology." *PRAWO i WIĘŹ 1* (44) (2023): 195-215:196.

original data, it stores its previous block's digital signature.[24] The blockchain received its name from these connected blocks.

Its advantage is that it is immutable and secure, decentralized, and distributed. One can have a quick response or unique encrypted code, which is a very effective way to identify fake products.[25] When a quick response code is scanned, or a unique code is entered, it directs the user to the blockchain containing the product information.[26] It provides the manufacturer and owner details to make the buyer's decision easier.

By using blockchain, users can exchange digital assets anonymously without needing to know and trust each other or a third-party in their transactions. Every time the ownership of the product changes, new transactions are sent to the blockchain. Therefore, preserving the history of a product makes the origins and its various points easier to identify. This method makes the transactions made in the pharmaceutical supply chain more transparent.[27] By using blockchain in the pharmaceutical industry, it is possible to observe the drug transactions that occur during the distribution process, and consumers can check the details of drugs purchased from vendors.

4. Limitations of Deploying Blockchain Technology in the Pharmaceutical Industry

After the growth and expansion of computer technologies and developments in the virtual space, the investigation of different levels of the dimensions of new technologies, including blockchain, as the core of innovations and their effects on societies have been considered. Blockchain can revolutionize the pharmaceutical industry by improving transparency and traceability, reducing costs, and preventing falsification and distortion of drug supply chain information from origin to destination.

However, their establishment in the pharmaceutical industry may require more knowledge, technical expertise, and initial costs.[28] For example, one of the primary weaknesses of such systems and technologies is its scalability limitations. As the number of transactions increases, the network can become congested, creating challenges in tracking and verifying pharmaceutical products

24. Hemmati, et al. "Identifying and Prioritizing the Barriers and Necessities of Applying Blockchain Technology in Auditing with a Fuzzy Delphi Approach." *Accounting and Auditing Management Knowledge* 11.44 (2022): 261-279:263.

25. Ishaan Singhal, Himanshu Singh Bisht, and Yogesh Sharma, "Anti-Counterfeit Product System Using Blockchain Technology", *International Journal for Research in Applied Science and Engineering Technology* 912, no. 31 (2021): 291-295:292.

26. Ijazul Haq, and Olivier Muselemu Esuka. "Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs." *International Journal of Computer Applications* 180.25 (2018): 8-12:9.

27. *Ibid*.

28. Prateek Pandey, and Ratnesh Litoriya, "Securing E-Health Networks from Counterfeit Medicine Penetration Using Blockchain", *Wireless Personal Communications* 117 (2021): 7-25.

in the supply chain.[29] High costs can also be an obstacle for users, especially in developing countries, or small-scale drug suppliers, which affects the widespread adoption of new solutions to combat drug counterfeiting.[30]

Another critical challenge for blockchain-based systems is adopting and integrating this technology throughout the pharmaceutical supply chain. Ensuring compliance with existing regulations can face uncertainty during system implementation. This is due to the fact that computer crimes, which are more commonly known as cybercrimes, have different judicial approaches.[31] Most crimes, such as hacking and DDoS attacks, target specific computers. In these cases, countries can claim jurisdiction based on the computer's location, the crime's effects, or the victim's nationality.[32]

One possible factor that leads to problems in estimating cybercrimes is the need for definitions and classification systems in the spectrum of cybercrimes.[33] This problem is exacerbated by cybercrime laws needing to be more systematic and uniform across jurisdictions.[34]

Therefore, in the discussion of compliance with existing regulations, while implementing blockchain-based systems and navigating regulatory requirements, data privacy laws, and industry standards, the solutions of these proposed systems may face challenges in the pharmaceutical sector. Security risks associated with smart contracts, such as coding errors or regulatory gaps, can compromise the data integrity of the pharmaceutical supply chain and lead to incidents of counterfeit drugs.

Therefore, the legal implementation of blockchain technology faces ambiguities and challenges, and must therefore be addressed. Discussions such as jurisdiction and privacy protection in the face of legal issues surrounding blockchain-based systems have legal gaps in adapting to national or international laws. While immutability is a valuable and critical feature of blockchain, it acts as a double-edged sword.

For example, in compliance with the European Union law, since the data

29. Gökalp, E., Gökalp, M. O., Çoban, S., & Eren, P. E. "Analysing Opportunities and Challenges of Integrated Blockchain Technologies in Healthcare. Information Systems: Research, Development, Applications, and Education", *11th SIGSAND/PLAIS Euro Symposium 2018, Gdansk, Poland, September 20, 2018, Proceedings* 11, 174-183:181.

30. Scott J. Shackelford,, and Steve Myers. "Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber peace", *Yale JL & Tech*. 19 (2017): 334

31. Sanna Kulevska, "Humanizing the Digital Age: A Right to Be Forgotten Online? An EU–US Comparative Study of Tomorrow's Privacy in Light of the General Data Protection Regulation and Google Spain v. AEPD." (2014):1-85:25.

32. Susan W Brenner,., and Bert-Jaap Koops. "Approaches to Cybercrime Jurisdiction." *J. High Tech. L.* 4 (2004): 1.

33. Kirsty Phillips, *et al*. "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." *Forensic sciences* 2.2 (2022): 379-398:394.

34. Susan W Brenner, and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction", *J. High Tech. L.* 4 (2004):40.

stored in the ledger cannot be deleted or altered (at least not easily), blockchain does not automatically comply with the European Union data protection rules; this is because the General Data Protection Regulation of the European Union provides the right to be forgotten.[35] At the same time, the Consumer Protection Act in the United States gives consumers the right to request the modification or deletion of their data. Therefore, judicial approaches differ in these circumstances.[36]

At this point, is there an international binding treaty to invoke? A critical international document related to the Internet is the Budapest Convention on Cybercrime (Cyberspace), also known as the Council of Europe Convention on Cybercrime. The Treaty establishes legal frameworks for combating cybercrime, including provisions on jurisdiction, extradition and mutual legal assistance between signatory countries.[37] Many countries have modelled their laws based on this Convention, but not all countries have ratified it. Therefore, it has no binding obligation. There are other scattered and non-binding documents, such as the Tallinn Manual, which was prepared by a group of international law experts and provides guidance on applying existing international laws in cyber operations, including issues related to government jurisdiction and responsibility in cyberspace.[38]

Other documents and treaties that create frameworks for dealing with judicial issues, cybercrimes, data protection and other legal aspects related to the Internet at the international level include the International Telecommunication Regulations by the International Telecommunication Union.

In general, the challenges facing this technology are a lack of clarity in terminology and lack of understanding of technology maturity, perceived risks in early adoption and possible disruption in existing industry procedures, lack of transparency in managing this technology, uncertainty about regulations, high costs, and lack of ensuring data integrity. These challenges include jurisdictional issues, cryptographic suites, privacy and data protection, and proper definition of liability.

In the following, the challenges related to the legal settings of blockchain technology are examined.

35. Right to be forgotten (RTBF) The right to be forgotten is a relatively new legal concept that has many implications for Internet policies, freedom of expression, and privacy; it is the right to remove people's private information from internet searches and other directories under certain conditions. This concept has been discussed and implemented in several jurisdictions, including Argentina, the European Union and the Philippines.

36. Sanna Kulevska, "Humanizing the Digital Age: A Right to Be Forgotten Online? An EU–US Comparative Study of Tomorrow's Privacy in Light of the General Data Protection Regulation and Google Spain v. AEPD", (2014):25.

37. Enver Buçaj, and Kenan Idrizaj. "The Need for Cybercrime Regulation on a Global Scale By The International Law and Cyber Convention." *Multidisciplinary Reviews* 8.1 (2025): 2025024.

38. https://ccdcoe.org/research/tallinn-manual/(2024/04/21)

5. Legal Settings of Blockchain Technology

5-1. Blockchain Jurisdiction

Jurisdiction on the Internet refers to the legal authority or control that a particular country or entity has over online activities and transactions within its borders or involving its citizens.[39] Due to the global nature of the Internet and the absence of physical borders in cyberspace, jurisdiction on the Internet is a complex and evolving issue. In cyberspace, the jurisdiction of the Internet is determined by registries that help identify the locations of parties in the network. The addresses of all users, *i.e.* the numbers assigned to every device that connects to the Internet, are registered in this network.[40]

One example of international Internet jurisdictions is the Uniform Domain Name Dispute Resolution Process, which sets the legal framework for resolving disputes between domain name registrants and third parties.[41] The Internet Corporation for Assigned Names and Numbers (ICANN) administers this procedure, along with the World Intellectual Property Organization (WIPO), but most states have limited jurisdiction over cybercrimes. Most crimes, such as hacking and cyberattacks, target specific computers and countries. [42] Jurisdiction is asserted based on the computer's location, the crime's evidence, or the victim's nationality.[43]

Therefore, one of the most significant legal challenges facing blockchain technology is the issue of jurisdiction. Because, as a decentralized ledger, blockchain nodes can span a large number of locations around the world, it makes it difficult to determine which has jurisdiction and also capable of resolving the disputes, as well as enforcing the contracts. This can create legal uncertainty and make enforcement of contracts, or resolving disputes difficult. However, this system must comply with all applicable legal and regulatory regimes. It also becomes difficult to determine the exact location of a transaction when that particular transaction is fraudulent or erroneous.

For example, if a smart contract is executed between two parties from different countries and subsequent to its execution a dispute arises, it needs to be clarified which court has jurisdiction to hear the case. Any transaction

39. Muhammad Qasim, Inam ur Rehman, and Hira Malik. "Cross-Border Enforcement of IP Rights in the Digital Era." *Law Research Journal* 3.3 (2025): 19-32:27.

40. Nanjwan Yale Damap, and Kangdim Dingji Maza Maza. "Jurisdictional Challenges in Cryptocurrency Disputes: Navigating the Legal Maze of a Borderless Technology." *African Journal of Stability and Development* (AJSD) 17.1 (2025): 132-160:154.

41. Sanna Kulevska, "Humanizing the Digital Age: A Right to Be Forgotten Online? An EU–US Comparative Study of Tomorrow's Privacy in Light of the General Data Protection Regulation and Google Spain v. AEPD", (2014):15.

42. Hacking: The term hacking means breaking into a computer system, and someone who has enough knowledge in fields such as programming and software can break into a system without having the necessary requirements and use its resources for himself. He is called a hacker.

43. Susan W Brenner, and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction", *J. High Tech. L.* 4 (2004):40.

stored on the blockchain could be in any jurisdiction in which a node of the network resides, resulting in many laws that may apply to the blockchain network.

In the discussion of personal jurisdiction, exercising jurisdiction in virtual space requires verifying the citizenship of the criminal or the victim, and identifying the criminal in this space depends on determining his ID,[44] which is the number assigned to every device that connects to the Internet.[45]

While individuals can easily fake their ID by using computer programs, verifying the criminal's citizenship in the nodes of a blockchain network and applying personal jurisdiction is impossible. Also, in the discussion of drug counterfeiting in the drug supply chain, when it is related to the crimes of different countries, for example, the production of goods in one country and distribution in another, it becomes difficult to determine the governing law of a blockchain-based system, especially if the system is in several jurisdictions.

The standards and rules governing a blockchain-based system are complex because blockchain technology is a new form of architecture of trust and choice.[46] In this new technology, the laws and regulations of different jurisdictions diverge, including on the basic principles of contracts and titles in those systems. What constitutes a valid blockchain-based contract in one country may be an invalid contract in another. To avoid this confusion, the law governing transactions should be predetermined by a governing system. This allows users to determine the validity of contracts and their rights and obligations. It would also be helpful to define a dispute resolution method acceptable to all parties involved.

5-2. Blockchain Legal and Criminal Liability

The challenges of legal and criminal liability in blockchain-based supply chains stems from its decentralized and immutable nature, which can complicate the attribution of responsibility and accountability for transactions and activities recorded on the blockchain. This challenge has implications for regulatory compliance, law enforcement, and addressing criminal activity in blockchain-based supply chains.

In blockchain, we face many nodes. In the pharmaceutical supply chain, we have partners who act as data controllers, but we need to know who enforces the legal obligations.[47] In such cases, a legal entity or an individual

44. Identification

45. Seyyed Yaser Ziyai, and Ehsan Shakibnejad, "Legislation in Cyberspace: the Approach of International Law and Iranian Law", *Journal of International Law*, 34(57): (2016):249-227:231.

46. Ziad Hussein, May A. Salama, and Sahar A. El-Rahman, "Evolution of Blockchain Consensus Algorithms: a Review on the Latest Milestones of Blockchain Consensus Algorithms", *Cybersecurity* 6, no. 1 (2023):1-30:5.

47. Renata Hrecska-Kovacs, "Health Law Implications of the Use of Blockchain Technology", *PRAWO i WIĘŹ*, 1 (44): (2023):195-215:204.

in the groups shall be designated as the data controller and the one competent to decide on liability issues.The use of blockchain technology in the pharmaceutical industry requires the participation of several stakeholders, including manufacturers, distributors, and healthcare providers. In a data breach or other security incident, it can be challenging to determine who is responsible for damages.

Decentralized autonomous organizations are independent and governed by pre-coded rules.[48] Thus, without human intervention, their information is recorded in the blockchain to execute smart contracts. This creates several legal issues for blockchain companies.

First, what legal status will be granted to such institutions? Are they automated legal contracts, software, or a legal entity such as a corporation? Do they have the power to file a lawsuit? Who will be responsible in case of violation of any of the rules? This is a similar dilemma when determining who should be held liable for wrongdoing by a pharmaceutical company. Do we need to establish similar legal principles to determine the responsibility of decentralized autonomous organizations or their creators? Regulatory bodies and courts will need help deciding such disputes.

For example, in *Google Spain v. Spanish Data Protection Agency*, the Court of Justice of the European Union ruled that a search engine can be responsible for protecting personal data on third-party websites accessible through its service.[49]

In this case, a Spanish man sued the Spanish Data Protection Agency, asking Google to remove links to a newspaper article about his debts from search results. Spain's data protection agency ordered Google to remove the links in favour of the man. Google appealed the decision, arguing that it is not responsible for the content of the links.[50] The Court of Justice of the European Union ruled in favour of the man, stating that Google is responsible for processing personal data that appears in search results.

The Court recognized that individuals have the right to request the removal of links to their personal information if that information is inaccurate, insufficient, irrelevant or excessive.[51] The ruling established the "right to be forgotten" principle, which allows people to request that certain information be removed from search results.

Likewise, in a public blockchain system, no-one is as quickly accountable

48. Olivier Rikken, Marijn Janssen, and Zenlin Kwee, "Governance Challenges of Blockchain and Decentralized Autonomous Organizations", *Information Polity* 24, no. 4 (2019): 397-417:398.

49. Isabella Shuxin Savela, "Generative AI & the Right to Erasure: Can GDPR's 'Right to Be Forgotten'Delete AI Outputs?", (2025):1-83:20

50. Ryan Lloyd , and Rebecca Umbach. "Right to Be Delisted? Attitudes Toward Delisting Public Interest Information." *Journal of Online Trust and Safety* 2.5 (2025):1-34:4.

51. Isabella Shuxin Savela, "Generative AI & the Right to Erasure: Can GDPR's 'Right to Be Forgotten'Delete AI Outputs?", (2025):1-83:25

as a search engine. In a private blockchain system with clear ownership and responsibility, regulators may expect those running the system to be accountable for the data added to the system by all network users.[52] The system owner can be likened to a search engine, someone who can distribute data through the blockchain. The system owner will be responsible for protecting this data despite not releasing the personal data itself.

Therefore, the issue of responsibility in the blockchain field is different from what we face in criminal and civil law. Consequently, the challenge of legal and criminal liability in a blockchain-based supply chain stems from the complexities of attributing responsibility, ensuring legal compliance, and addressing criminal activity in a decentralized and immutable system. Addressing these challenges requires regulatory clarity and regulatory frameworks that accommodate blockchain technology.

5-3. Protection of Intellectual Property in Blockchain

Blockchain technology's decentralized and transparent nature can affect the ownership, management and enforcement of intellectual property rights in supply chain transactions and processes. This challenge has implications for protecting innovation, preventing unauthorized use of intellectual property, and ensuring fair competition in blockchain-based supply chains. It highlights the challenges of managing and protecting intellectual property assets in blockchain-based supply chains, such as patents, trademarks, and copyrights. Blockchain technology can facilitate the safe and transparent management of intellectual property rights through smart contracts and decentralized registries.[53] It can enable secure and efficient transactions, reduce the risks of fraud and counterfeiting, and increase transparency and traceability in supply chain processes.

However, protecting intellectual property rights in blockchain-based supply chains requires the creation of legal frameworks, standards, and best practices that address data privacy, confidentiality, and ownership of intellectual property assets.

5-4. Data Security and Privacy

The challenges of protecting privacy and data security in blockchain-based supply chain applications are discussed, particularly in ensuring the confidentiality and integrity of sensitive information, such as product provenance, transaction details, and supply chain data.

For example, if a copy of personal data is made in Malaysia, does this

52. Salmon, J. and G. Myers, "Blockchain and associated legal issues for emerging markets", *Open Knowledge Repository beta, Report Series EM Compass Notes,* http://hdl.handle.net/10986/31202 (2023/11/12). Mobilizing Capital for Sustainability in Emerging Markets International Finance Corporation, Washington, DC: (2019). 1-8:6.

53. K. Tomasch, "Trade and Supply Chain Finance", *Global Trade*. (2024). see: https://iccwbo.org/global-insights/global-trade/trade-and-supply-chain-finance/ (2024/04/21). p:1.

mean the data has been "transferred" to Malaysia for the Privacy Act? In the sense that data may be transferred to a node anywhere, data placed on a public blockchain is similar to data posted on the public Internet.

The reasoning of the European Court of Justice in the *Lindqvist* case applies to this case. The Gotha Court of Appeal (Sweden) referred the case to the European Court of Justice for a preliminary ruling on questions related to the scope and interpretation of the European Data Protection Directive. This case was related to the criminal proceedings against Mrs Lindqvist,[54] who was accused of violating Swedish laws regarding the protection of personal data by creating a web page containing the information of her colleagues without their consent.[55]

By the same token, it must be ensured that the data of a blockchain is not transferred to any jurisdiction in which a node exists and does not violate that jurisdiction's privacy regulations. In the author's opinion, addressing privacy and security risks in blockchain-based supply chains requires implementing privacy protection mechanisms, secure identity management solutions, and cybersecurity measures to protect sensitive data from unauthorized access, manipulation, and disclosure.

5-5. Blockchain-Based Smart Contracts

Smart contracts are pre-written computer codes. The terms of the contract are defined based on "if" and "else." When specified criteria are met, blockchain-based contracts are executed automatically without the need for any intermediary to confirm the transaction.[56] This raises questions about enforceability, applicable law, and jurisdiction. Software developers may be responsible for part of the written code that results in customer losses. This can be caused by code malfunctioning or behaviour not intended by the parties to the transaction.

In addition, public blockchains in decentralized autonomous organizations can be subject to virtual attacks. Smart contracts raise issues related to contract formation requirements, purpose, and interpretation of contractual terms in a code-based agreement. Therefore, ensuring smart contracts' legal validity and enforceability requires addressing issues related to contract law and electronic signatures and recognizing blockchain records as evidence in

54. Bodil Lindqvist

55. Salmon, J. and G, Myers "BlockChain and Associated Legal Issues for Emerging Markets", *Open Knowledge Repository beta, Report Series EMCompass Notes,* http://hdl.handle.net/10986/31202 (2023/11/12). Mobilizing Capital for Sustainability in Emerging Markets International Finance Corporation, Washington, DC: (2019). 1-8:6.

56. Markus Klems, Jacob Eberhardt, Stefan Tai, Steffen Härtlein, Simon Buchholz, and Ahmed Tidjani, "Trustless Intermediation in Blockchain-Based Decentralized Service Marketplaces", *In Service-Oriented Computing*: *15th International Conference, ICSOC 2017*, Malaga, Spain, November 13–16, 2017, Proceedings, pp. 731-739. Springer International Publishing, (2017):3.

legal proceedings.

Among the considerations expressed for smart contracts, it is impossible to check the validity of general principles such as good faith, benefit, satisfaction or reasonableness, mainly in codes. That is, the essential elements of civil law have a limited ability to assert themselves in the automatic execution of smart contracts during their implementation.

Another legal issue in smart contracts is whether such documents can be suspended or their content invalidated. Of course, the algorithms of the suspension program can be easy or challenging depending on the nature of the programming conditions. For example, it becomes more difficult to understand at which stage the suspension should take place in each subject and according to which civil law.

Based on this, the blockchain-based dispute resolution model has some significant uncertainties. Due to the existing ambiguities, resolving the dispute through predetermined codes may cause several problems. In unforeseen circumstances, these technical rules may harm the parties' interests. Resolving a private blockchain-based arbitration without any third-party involvement for a wide area of law seems complicated.

Also, requesting and accepting transactions is another significant issue that should be addressed. In most smart contracts the buyer makes the payment, which is held in a safe place until the seller releases the goods or cryptocurrency. After publishing the goods or virtual assets, the seller is automatically paid. This issue raises the issue of product demand and acceptance. Traditional contracts often contain provisions about the standard and quality of the goods, and the buyer is only considered to have accepted the goods once he has had a reasonable opportunity to check their compliance with the contract.[57] The smart contract must specify which rules are applicable, whether there is a reason to deny the product, and at what stage the request and acceptance of the product are made. This can be seen in the blockchain-based systems used in the pharmaceutical industry in matters of business transactions and drugs in the supply chain.

The provisions of contracts usually cover events such as wars, epidemics, natural disasters, wildfires, or anything beyond the control of ordinary people and the like.[58] However, in the case of a blockchain-based system, legal issues may arise. There are others, such as a malfunctioning smart contract, issues related to the transfer of underlying cryptocurrencies, parties' access to the blockchain, etc., which should be clearly stated. Are such events included in the scope of force majeure? An exception may also be made to this provision that the parties cannot claim the protection of force

57. John Felemegas, "The United Nations Convention on Contracts For The International Sale of Goods: Article 7 and Uniform Interpretation", *PhD diss., University of Nottingham*, (2000):1.

58. Safai, Seyyed Hossein, "Force Majeure Overview in Natural Law and International Law and International Commercial Contracts", *International Legal Journal*, 3(3), (1985) 111-154:118.

majeure provisions for issues arising from their failure to maintain appropriate industry safeguards. In this case, developing guidelines and complying with existing laws is necessary to implement smart contracts in a decentralized and automated system to facilitate safe and efficient supply chain transactions.

6. Blockchain Governance: A Key Factor

Blockchain governance is defined as achieving direction, control, and coordination of stakeholders in a blockchain network. It is multifaceted and complex due to its decentralized nature and the rules and mechanisms that are automatically implemented.[59] This governance consists of two layers: the first layer is technical and social tools for decision-making at various individual and social levels, and the second layer is related to the participants, roles, rights, responsibilities, laws, businesses, technology and regulatory aspects of the blockchain system in its entire life cycle.[60]

Beck, back in 2018 proposed a governance framework that extracts three key dimensions of governance: a) decision-making about the development of rules that give individuals the power to control governance, b) accountability, which is the extent to which stakeholders can be held accountable for their actions, and c) incentives that emphasize the motivation of stakeholders to take action.[61]

Blockchain governance combines the degree of incentive alignment, centralization in decision-making rules, and the level at which technical or institutional accountability is exercised. Also, one important legal issue is that these models must specify the rules and regulations applicable to the blockchain platform.

The functional nature of the blockchain platform means that the relationship between the blockchain network, the network operator (if any) and its participants needs to be documented through legally enforceable contracts. It is also necessary to carefully assess the nature and activities of a blockchain network and its participants and determine where that platform and its participants should be placed in the regulatory landscape.[62] This issue is important for assigning responsibility to the network nodes at which point of jurisdiction they are located. Blockchain governance directly affects

59. Kevin Werbach, Primavera De Filippi, Joshua Tan, and Gina Pieters, "Blockchain Governance in the Wild." *Cryptoeconomic Systems* .3.1(2024).

60. Gabriella Laatikainen, Mengcheng Li, and Pekka Abrahamsson. "A System-Based View of Blockchain Governance." *Information and Software Technology* 157 (2023): 107149.

61. Rowan van Pelt, *et al*. "Defining Blockchain Governance: A Framework for Analysis and Comparison." *Information Systems Management* 38.1 (2021): 21-41:27.

62. Marvin Hanisch, Curtis M. Goldsby, Nicolai E. Fabian, and Jana Oehmichen, "Digital Governance: A Conceptual Framework and Research Agenda,", *Journal of Business Research* 162 (2023): 6.

monitoring factors such as automatic fraud detection and transparent operational data. The governance model should be designed to ensure that the network is secure, reliable and transparent and to ensure compliance with laws and regulations.

Conclusion

Because globally active blockchain networks involve multiple parties from different jurisdictions, regulators face challenges applying existing laws and regulations to blockchain-based supply chain activities. Lack of transparency in jurisdiction can create regulatory gaps, jurisdictional disputes, and conflicts between legal frameworks.

The challenge of legal and criminal liability in a blockchain-based supply chain stems from the complexities of attributing responsibility, ensuring legal compliance, and addressing criminal activity in a decentralized and immutable system. Also, protecting intellectual property rights in blockchain-based supply chains requires the creation of legal frameworks, standards, and best practices that address data privacy, confidentiality, and ownership of virtual assets. Protecting privacy and data security in the blockchain-based supply chain requires ensuring compliance with data protection regulations, preventing unauthorized access to sensitive information, and addressing privacy and security risks in a decentralized and transparent system.

As can be seen, most of the challenges are due to the need for clearer and more unified regulations due to the nascent nature of blockchain technology. Therefore, one of the possible solutions to solve the legal gaps of blockchain technology is to create clear and comprehensive regulations and guidelines for its use. This can create a more consistent and predictable regulatory environment. Overall, a collaborative approach involving governments, regulators, pharmaceutical industry professionals, and legal experts is critical to addressing the legal loopholes of blockchain technology and ensuring its responsible and ethical use.

However, to achieve this, the biggest issue that blockchain needs to pay attention to is its governance. Blockchain governance in a supply chain refers to several factors related to decision-making, accountability, and coordination among network participants. Blockchain technology's decentralized and distributed nature requires a governance framework that ensures transparency, consensus, and compliance with laws and regulations. This governance model should be aimed at solving the legal and regulatory challenges related to complying with the regulations in the standards and issues related to the laws governing the blockchain-based system, and this is important in the issue of combating drug counterfeiting in the pharmaceutical industry in light of the efforts of the legislators. They must be deeply connected to the IT domain to understand and facilitate system development within existing regulatory frameworks.

Legislators should define conditions according to the nature of distributed data storage in blockchain.

These conditions should be codified in areas such as the protection of intellectual property rights and data records, creating access guarantees, laws governing blockchain-based platforms and smart contracts, and determining the law governing transactions in counterfeiting and pharmaceutical fraud in the circulation of drugs. These codes must be defined in the technical and social layers of blockchain governance according to the specific mechanisms of each layer.

Through the above codes, it is possible to protect health data in pharmaceutical products and complete monitoring of the drug supply chain to prevent drug counterfeiting. Legal and information technology professionals should work closely together to determine the type of blockchain governance, and first of all, different standards should be established for interdisciplinary interactions.

References

Persian Sources

- Articles

1. Ghanbari, Mohammad Ali, Afsaneh Ghanbari, and Kourosh Delpasand, "The Inclusion of Traditional and Complementary Medicine in the Strategy of the United Nations and the World Health Organization". *Journal of Medical History*, 11 (41), (2018).
2. Mirkarimi, Pejman, Seyyed Baqer Mir Abbasi, and Maryad Moradi, "Investigating the Role and Position of Intellectual Property Rights in the General International Law System". *Iranian Political Sociology Monthly*. 5 (11), (1401).
3. Niavarani, Saber, Ehsan Javed, "The Right of Access to Essential Medicines in the Framework of the TRIPS Agreement and the Challenge of Protecting the International Human Right to Health". *International Legal Journal*. 33 (54) (2015).
4. Safai, Seyyed Hossein. "Force Majeure Overview in Natural Law and International Law and International Commercial Contracts". *International Legal Journal*, 3(3), (1985).
5. Ziyai, Seyyed Yaser and Ehsan Shakibnejad, "Legislation in cyberspace: the approach of international law and Iranian law". *Journal of International Law*, 34(57): (2016)

English Sources

- Book

1. Gopakumar, K. M., and Sangeeta Shashikant. *Unpacking the Issue of Counterfeit Medicines*. Penang, Malaysia: Third World Network, (2010).

2. World Health Organization. *International Health Regulations* (2005). *World Health Organization*, (2008).

- Articles

1. Alla, Sujatha, Unal Tatar Leili Soltanisehat, and Omer Keskin, "Blockchain Technology in Electronic Healthcare Systems." In IIE Annual Conference. Proceedings. *Institute of Industrial and Systems Engineers (IISE*), 2018.
2. Brenner, Susan W., and Bert-Jaap Koops. "Approaches to Cybercrime Jurisdiction." *J. High Tech*. L. 4 (2004).
3. Buçaj, Enver, and Kenan Idrizaj. "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention." *Multidisciplinary Reviews* 8.1 (2025).
4. CESCR, General Comment No. 14, para. 35. *Committee on Economic, Social & Cultural Rights (CESCR)*, "The Right to the Highest Attainable Standard of Health", (article 12 of the ICESR), General Comment, No.14. 2000.
5. Nanjwan Yale Damap, and Kangdim Dingji Maza Maza. "Jurisdictional Challenges in Cryptocurrency Disputes: Navigating the Legal Maze of a Borderless Technology." *African Journal of Stability and Development (AJSD)* 17.1 (2025).
6. El Feky, Mahmoud Farouk. "Using New Digital Anti-Counterfeiting Technologies to Protect the Egyptian Pharmaceuticals Packages Against Counterfeiting." *International Design Journal* 10.3 (2020).
7. Felemegas, John, "The United Nations Convention on Contracts for the International Sale of Goods: Article 7 and Uniform Interpretation." *PhD diss., University of Nottingham*, (2000).
8. Gökalp, E., Gökalp, M. O., Çoban, S., and Eren, P. E, "Analysing Opportunities and Challenges of Integrated Blockchain Technologies in Healthcare Information Systems: Research, Development, Applications, Education". *11th SIGSAND/PLAIS Euro Symposium 2018*, Gdansk, Poland, September 20, 2018, Proceedings 11, (2018).
9. Hanisch, Marvin, Curtis M. Goldsby, Nicolai E. Fabian, and Jana Oehmichen, "Digital Governance: A Conceptual Framework and Research Agenda." *Journal of Business Research* .162 (2023).
10. Hasan, Khondker Shajadul, and Shezad Rouf Khondker. "Utilizing Blockchain Technology in Cyber Security to Secure Pharmaceutical Industry Supply Chain." *Conference Paper*. (2022).
11. Haq, and Olivier Muselemu Esuka. "Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs". *International Journal of Computer Applications* 180, no. 25 (2018).
12. Hogerzeil, Hans V. "Essential Medicines and Human Rights: What Can They Learn From Each Other?". *Bulletin of the World Health Organization* 84 (2006).

13. Hrecska-Kovacs, Renata., "Health Law Implications of the Use of Blockchain Technology." *PRAWO i WIĘŹ*, 1 (44) (2023).

14. Hussein, Ziad, May A. Salama, and Sahar A. El-Rahman. "Evolution of Blockchain Consensus Algorithms: a Review on the Latest Milestones of Blockchain Consensus Algorithms". *Cybersecurity* 6, no. 1 (2023).

15. Klems, Markus, Jacob Eberhardt, Stefan Tai, Steffen Härtlein, Simon Buchholz, and Ahmed Tidjani. "Trustless Intermediation in Blockchain-Based Decentralized Service Marketplaces." In Service-Oriented Computing: *15th International Conference, ICSOC 2017*, Malaga, Spain, November 13–16, 2017, Proceedings, Springer International Publishing, (2017).

16. Kulevska, Sanna, "Humanizing the Digital Age: A Right to Be Forgotten Online? An EU–US Comparative Study of Tomorrow's Privacy in Light of the General Data Protection Regulation and Google Spain v. AEPD." (2014).

17. Laatikainen, Gabriella, Mengcheng Li, and Pekka Abrahamsson. "A System-Based View of Blockchain Governance." *Information and Software Technology* 157 (2023).

18. Lloyd, Ryan, and Rebecca Umbach. "Right to Be Delisted? Attitudes Toward Delisting Public Interest Information." *Journal of Online Trust and Safety* 2.5 (2025).

19. Litchfield, A., and Arshad Khan. "A Review of Issues in Healthcare Information Management Systems and Block Chain Solutions." (2019).

20. Maaz, Muhammad, and Tahir Ali. "How Counterfeits Goods Are Destroying Brand Reputation." *Journal of Engineering and Economic Development* 6, no. 2 (2020).

21. Pandey, Prateek, and Ratnesh Litoriya. "Securing E-health Networks From Counterfeit Medicine Penetration Using Blockchain". *Wireless Personal Communications* 117 (2021).

22. Pathak, Ranjana, *et al*. "Tackling Counterfeit Drugs: the Challenges and Possibilities". *Pharmaceutical Medicine* 37.4 (2023).

23. Pelt, Rowan van, *et al*. "Defining Blockchain Governance: A Framework for Analysis and Comparison." *Information Systems Management* 38.1 (2021).

24. Phillips, Kirsty, *et al.* "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies." *Forensic Sciences* 2.2 (2022).

25. Qasim, Muhammad, Inam ur Rehman, and Hira Malik. "Cross-Border Enforcement of IP Rights in the Digital Era." *Law Research Journal* 3.3 (2025).

26. Rikken, Olivier, Marijn Janssen, and Zenlin Kwee. "Governance Challenges of Blockchain and Decentralized Autonomous Organizations." *Information Polity* 24, no. 4 (2019).

27. Salmon, J. and G. Myers. "Blockchain and Associated Legal Issues for Emerging Markets". *Open Knowledge Repository beta, Report Series EM Compass Notes*, http://hdl.handle.net/10986/31202 (2023/11/12). Mobilizing Capital for Sustainability in Emerging Markets International Finance Corporation, Washington, DC: (2019).

28. Savela, Isabella Shuxin. "Generative AI & the Right to Erasure: Can GDPR's 'Right to Be Forgotten 'Delete AI Outputs?" (2025).

29. Shackelford, Scott J., and Steve Myers. "Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace". *Yale JL & Tech*. 19 (2017).

30. Silveira, Alice Bryk. "Risk-Creating Industries' Obligation to the Right to Health". *Business and Human Rights*. Brill Nijhoff, (2025).

31. Singhal, Ishaan, Himanshu Singh Bisht, and Yogesh Sharma. "Anti-Counterfeit Product System Using Blockchain Technology." *International Journal for Research in Applied Science and Engineering Technology* 912, no. 31 (2021).

32. Sirrs, Christopher J. "Fluid Fakes, Contested Counterfeits: The World Health Organization's Engagement with Fake Drugs, 1948–2017." *Medicine Anthropology Theory* 10.3 (2023).

33. Tomasch, K. "Trade and Supply Chain Finance". *Global trade*. (2024). see: https://iccwbo.org/global-insights/global-trade/trade-and-supply-chain-finance/ (2024/04/21).

34. Tseng, Jen-Hung, Yen-Chih Liao, Bin Chong, and Shih-wei Liao. "Governance on the Drug Supply Chain via Gcoin Blockchain." *International Journal of Environmental Research and Public Health* 15, no. 6 (2018).

35. Werbach, Kevin, Primavera De Filippi, Joshua Tan, and Gina Pieters. "Blockchain Governance in the Wild." *Crypto economic Systems* .3.1 (2024).

36. Zhang, Dingyuan, and Caiqian Cheng. "AI-Enabled Product Authentication and Traceability in Global Supply Chains." *Journal of Advanced Computing Systems* 3.6 (2023).

37. Zhu, Peng, Jian Hu, Yue Zhang, and Xiaotong Li. "A Blockchain Based Solution for Medication Anti-Counterfeiting and Traceability." *Ieee Access* 8 (2020): 184256-184272: 184260.