Наукові записки НаУКМА
Юридичні науки 16 (2025)

NaUKMA Research Papers
Law 16 (2025)

СТАТТЯ

ARTICLE

DOI: 10.18523/2617-2607.2025.16.88-106
UDC 341.9:347.4+346.3:339.5

Liubov Logush
Candidate of Science of Law, Associate Professor
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
https://orcid.org/0000-0003-4753-1768
l.logush@ukma.edu.ua

Maksym Baryshov
Second-year master's student
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
https://orcid.org/0009-0003-8562-2326
maksym.baryshov@ukma.edu.ua

RISK ALLOCATION IN BLOCKCHAIN-BASED LICENSING AGREEMENTS FOR DUAL-USE TECHNOLOGIES AT THE INTERSECTION OF UKRAINIAN AND EU JURISDICTIONS

Abstract

The article explores the application of blockchain for risk allocation in cross-border licensing agreements of dual-use technologies under Ukrainian and EU legal frameworks.

The first section analyses blockchain technology from both technical and legal perspectives. It outlines the operational principles of the most widely used consensus mechanisms in supply chain management and identifies key threats inherent in each of them. The analysis includes the most common types of attacks targeting blockchain infrastructure. The criteria of suitable consensual mechanisms for dual-use technology transactions are determined. The section further focuses on the theoretical concept and grounds for blockchain implementations in licensing agreements, including smart contracts, blockchain-based supply chain management, and dispute resolution. The role of smart contracts in licensing agreements is examined in terms of their implementation within the operational lifecycle of commercial entities. Considering supply chain management, possible approaches to blockchain adoptions are presented. Regarding dispute resolution, contemporary methods in the digital realm are described.

The second section examines the integration of blockchain technology for risk allocation in cross-border licensing agreements in the EU market. It defines the concepts of risk and its allocation between contracting parties, from economic and legal perspectives. Two categories of risks are distinguished: those inherent in licensing agreements and those specific to the dual-use technology sector. The first category addresses risks associated with conflict-of-law issues, counterfeiting, and royalty formation. The limits of blockchain-based risk allocation are discovered in light of the exclusive-jurisdiction rule. Subsequently, the adoption of blockchain-based SCM is studied through the lens of the allocation of counterfeiting risk. A similar approach is applied to the risk of information asymmetry. The second category of risks concerns export controls and sanctions. The EU regulatory frameworks governing the relevant fields are examined. Contemporary examples of SCM implementations used to allocate export-control and sanctions risks are analysed. Both risks can be allocated between contractual parties through blockchain-based SCM.

The study results in the development of a risk allocation matrix using blockchain technology.

Keywords: blockchain, risk allocation, cross-border transactions, licensing agreements, dual-use technologies.

Analysis of recent research and publications

The number of available consensus types is skyrocketing, although a few have already proved themselves in market applications.[1] Most of these mechanisms remain vulnerable to different kinds of attacks, including clone attacks,[2] the Sybil attack,[3] the 51% attack,[4] etc. At the same time, hybrid models that combine different mechanisms have been proposed to mitigate these vulnerabilities and reduce the risk of third-party interference with sensitive information.[5] However, their effectiveness still lacks sufficient empirical validation.

Although a substantial body of scholarship has already explored various uses of blockchain – including smart contracts,[6] stablecoins for transactions,[7] blockchain-based supply chain management,[8] and dispute resolution,[9] – its application to licensing agreements at the intersection of Ukrainian and EU jurisdictions remains underexplored.

Theories about legal risks have been extensively developed in different fields of law, including the law of sale,[10] international IP contracting implications,[11] governmental procurement,[12] International Power Projects,[13] e-commerce.[14] Moreover, a solid background is given in the context of the risks inherent in technology licensing agreements, which arise out of the exclusive jurisdiction rule,[15] governing law principles,[16] counterfeiting,[17] enforcement of IP rights,[18] royalty formation,[19] contract formation under asymmetric information,[20] and a lack of transparency regarding the value of technology.[21]

Furthermore, a number of risks have been developed in the academic domain in the field of technology transfer, including its licensing and distribution. In particular, we will focus on those involving export[22] and sanctions[23] controls over the distribution of technologies. At the same time, the application of these doctrines to risk allocation in cross-border licensing agreements is limited. Although several studies analyse distributed ledger applications in the supply chains of dual-use and military technologies, such as the nuclear material chain,[24] their use remains limited to the national level and does not consider the implementation of licensing

---

1 Bahareh Lashkari and Petr Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," *IEEE Access* 9 (2021): 43646.
2 Parinya Ekparinya et al., "The Attack of the Clones Against Proof-of-Authority," 5–6, 15, arXiv preprint arXiv:1902.10244 (2019).
3 J. R. Douceur, "The Sybil Attack," in *Lecture Notes in Computer Science*, eds. P. Druschel, F. Kaashoek, and A. Rowstron, Vol. 2429 (Springer, 2002), 1, 5.
4 Nur Arifin Akbar et al., "Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses," *Future Internet* 13, no. 11 (2021): 7, https://doi.org/10.3390/fi13110285.
5 Fan Yang et al., "Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism," *IEEE Access* (2019): 7, https://doi.org/10.1109/ACCESS.2019.2935149.
6 C. Poncibò, "The Digitalization of Contracts in International Trade and Finance: Comparative Law Perspectives on Smart Contracts," in *Digitalization and Firm Performance* (Springer International Publishing, 2022), 134–5.
7 Francesco Giumelli, "A Comprehensive Approach to Sanctions Effectiveness: Lessons Learned from Sanctions on Russia," *European Journal on Criminal Policy and Research* 30, no. 2 (2024): 402.
8 Javed Aslam et al., "Factors Influencing Blockchain Adoption in Supply Chain Management Practices: A Study Based on the Oil Industry," *Journal of Innovation & Knowledge* 6, no. 2 (2021): 36.
9 Yigit Efe Dincer, "Arbitration in the Age of Blockchain" (Master's thesis, Université de Montréal, 2023).
10 L. S. Sealy, "Risk in the Law of Sale," *Cambridge Law Journal* 31, no. 1 (1972): 226.
11 Miquel dels Sants Mirambell Fargas, "Economics of Arbitrability in International IP Contracting," *Journal of Law and Commerce* 37, no. 2 (2019): 226, https://doi.org/10.5195/jlc.2019.164.
12 *Risk Allocation and Pricing Approaches: Guidance Note, prepared by Government Commercial Function* (London: GCF, 2021), 4–6, https://assets.publishing.service.gov.uk/media/60a388a9e90e07357baa83da/Risk_allocation_and_pricing_approaches_guidance_note_May_2021.pdf.
13 John G. Mauel, "Common Contractual Risk Allocations in International Power Projects," *Columbia Business Law Review* 1996, no. 1 (1996): 38.
14 Roger Reinsch, "E-Commerce: Managing the Legal Risks," *Managerial Law* 47, no. 1/2 (2005): 177.
15 Benedetta Ubertazzi, *Exclusive Jurisdiction in Intellectual Property* (Tübingen: Mohr Siebeck, 2012), 10.
16 Katharina Kaesling, "The European Patent with Unitary Effect – A Unitary Patent Protection for a Unitary Market?," *UCL Journal of Law and Jurisprudence* 2 (2013): 94–5.
17 Naif Alzahrani, and Nirupama Bulusu, "Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (2018), 35, https://doi.org/10.1145/3211933.3211939.
18 Vladimir Bastidas Venegas, "Intellectual Property Rights, Enforcement Costs and EU Competition Law," *Journal of Antitrust Enforcement* 11, issue supplement_1 (2023): i38, https://doi.org/10.1093/jaenfo/jnac027.
19 Stefano Colombo et al., "Patent Licensing and Capacity in a Cournot Model," *Review of Industrial Organization* 62, no. 1 (2023): 47.
20 Nancy T. Gallini and Brian D. Wright, "Technology Transfer under Asymmetric Information," *The RAND Journal of Economics* 21, no. 1 (1990): 150.
21 Rudi Bekkers et al., "Overcoming Inefficiencies in Patent Licensing: A Method to Assess Patent Essentiality for Technical Standards," *Research Policy* 51, no. 10 (2022): 47, https://doi.org/10.1016/j.respol.2022.104590.
22 Ester Sabatino, "Arms Supplies to Ukraine: Does the European Arms Export Control System Need Revision?," *EU Non-Proliferation and Disarmament Consortium* 89 (2024): 4.
23 Stefano Silingardi, "The EU 11th and 12th Packages of Sanctions Against Russia: How Far is the EU Willing to Go Extraterritorially?," *Global Trade and Customs Journal* 19, no. 7/8 (2024): 8–9.
24 Cindy Vestergaard, "Streamlining Export Controls with Blockchain (블록체인을 통한 수출통제의 효율화)," Professional Report. Stimson Center, Korean Security Agency of Trade and Industry (무역안보 저널), *Trade & Security* 1 (June 2021): 45.

agreements within these chains. Meanwhile, more comprehensive applications, such as Louis Vuitton's AURA platform, do not focus on technology transfer, but rather on the supply chain of physical goods.[25]

Therefore, this research aims to lay a foundation for resolving the question of whether blockchain-based licensing agreements is a protected means of technology transfer.

Introduction

Blockchain technology has all the prerequisites to become a key instrument for risk allocation in cross-border transactions, particularly in licensing agreements concerning dual-use technologies.

Blockchain technology has significantly transformed the way transactions are conducted. It enhances security, helping build trust between contract parties. In the context of EU-Ukraine relations it could play a key role in advancing technological exchange.

Licensing agreements are strategically important. By entering new markets licensors can set de facto standards for complementary products and benefit from subsequent sales, which is especially relevant for inventors: "...who lack the resources, experience and ability to establish a product on the market".[26] Licensing revenues might stimulate technological development, Ukraine's economy and its defence industrial complex. Hence, blockchain adoption to IP management[27] is crucial for both increasing the effectiveness of transactions, and enhancing public security.

Moreover, Ukraine and the EU are facing the challenges of a new world order. The fragility of security guarantees for Ukraine concerning sovereignty and territorial integrity, which tend to be rather political assurances, makes the development of military and dual-use technologies the only viable guarantee. To achieve financial independence from external sources, Ukraine's defence industry must commercialise its inventions, for which the EU market is one of the most suitable.

1. Blockchain as an Instrument of Risk Allocation in Cross-border Transactions

The most accepted definition of blockchain technology simply refers to a chain of blocks in which a distributed ledger is recorded, cryptographically protected, and enforced by a consensus mechanism.[28]

Blockchain as a distributed ledger technology (**DLT**), has "no central authority that controls, verifies, and validates these transactions".[29] Moreover, the blockchain database relies on records that "are collectively managed by a peer-to-peer network comprised of computers (known as "peers" or "nodes"), often scattered across the globe".[30] Additionally, blockchain technology is considered a trust protocol that enables unknown parties to rely on each other's obligations without intermediaries.[31]

Gönenç Gürkaynak suggests dividing the definition of blockchain into three fields: technical, business, and legal. From the technical point of view, blockchain is considered a: "[b]ack-end database that maintains a distributed ledger, openly". Meanwhile, the business definition considers blockchain an: "exchange network for moving value between peers". Finally, from the legal perspective blockchain is defined as: "a transaction validation mechanism, not requiring intermediary assistance".[32]

Consensus Mechanisms. The key element in terms of information security is to achieve a consensus on what should be stored in the DLT. Bahereh Lashkar and Petr Musilek define the consensus mechanism as a process that: "is utilised to preserve agreement among the nodes in the network…"[33]

Consensus between DLT participants ensures that all replicas of the blocks created by users simultaneously are identical and verified. In conclusion, the criteria for assessing the reliability of consensus mechanisms are their capability to ensure that: "all nodes will contribute to an identical, consistent, and valid output."[34]

---

25 Ibid.

26 Sebastian-Ioan Ene, "Intellectual Property Strategy – With main focus on patents and licensing of patents" (Master's thesis, NTNU, 2014), 41.

27 Gonenc Gurkaynak et al., "Intellectual Property Law and Practice in the Blockchain Realm," *Computer Law & Security Review* 34, no. 4 (2018): 857.

28 Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," *White paper* 3, no. 37 (2014): 6.

29 Poncibò, "The Digitalization of Contracts in International Trade and Finance," 132.

30 Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018), 2.

31 Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (New York: Portfolio / Penguin, 2016), 22.

32 Gurkaynak et al., "Intellectual Property Law and Practice in the Blockchain Realm," 848.

33 Lashkari and Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," 43622.

34 Ibid., 43624–5.

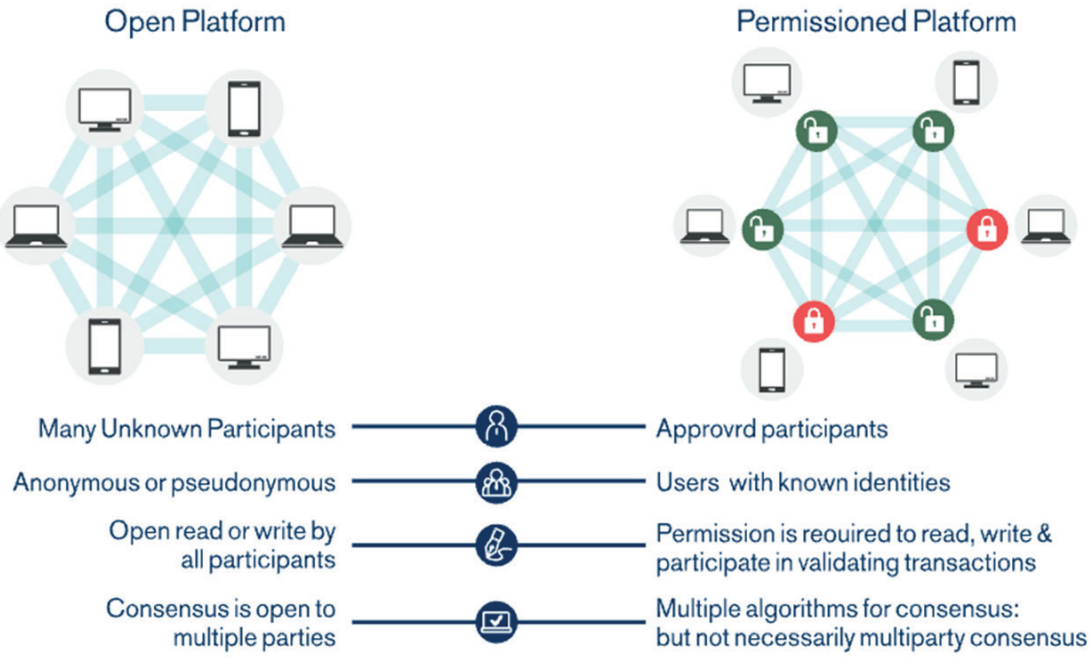

Figure 1. Comparison of public and permissioned consensus mechanisms [35]

On the first layer, there are two types of the consensus mechanisms: public and permissioned, as shown in Figure 1. A public blockchain allows any participant to create a node and consequently validate or reject underlying transactions. In contrast, a permissioned blockchain operates within a private network, where nodes can only be created with an administrator's authorisation. Some authors consider mixed types of blockchain, which combine features of both public and permissioned models.[36]

The number of consensus mechanisms is growing rapidly.[37] While different mechanisms suit different purposes depending on the field of application, this study focuses only on those applicable to supply chain management (**SCM**). According to market-based evaluation, four consensus models are the most reliable for SCM: Proof of Authority (**PoA**), Proof of Stake (**PoS**), Delegated Proof of Stake (**DPoS**), and Proof of Work (**PoW**).[38] Meanwhile, hybrid mechanisms should also be considered.

PoA is a permissioned consensus mechanism that involves authorised participants in the validation process. Shashank Joshi describes the PoA as "…a regulated or permissioned consensus protocol… that aims to reach a consortium through authorised nodes or validators. In this protocol, the reputation of the sealer is at stake…"[39]

On the one hand, PoA consume fewer resources, has better efficiency due to its centralised reputation-based approach, and is faster and more reliable at scale. On the other hand, PoA has several disadvantages that undermine its capacity to effectively maintain the SCM of dual-use inventions. It has insufficient protection against malicious activities and unauthorised external involvement, which creates the risk of third-party interference in the blockchain network. The level of its security has not been properly assessed.[40] Clone attacks[41] and Sybil attacks[42] are major vulnerabilities of this mechanism. PoA is not applicable for licensing agreements of dual-use technologies in cases where parties cannot rely on a trusted identification authority.

PoS is a consensus mechanism which relies solely on the legitimacy power of the data stored in the blockchain as enforced by society.[43] The mechanism of PoS block validation is described as follows: "users

35 Vestergaard, "Streamlining Export Controls with Blockchain," 42.
36 Gurkaynak et al., "Intellectual Property Law and Practice in the Blockchain Realm," 848.
37 Lashkari and Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," 43646.
38 Ibid.
39 Shashank Joshi, "Feasibility of Proof of Authority as a Consensus Protocol Model," arXiv preprint arXiv:2109.02480 (2021), 2.
40 Ekparinya et al., "The Attack of the Clones Against Proof-of-Authority," 1.
41 Ibid., 5–6, 15.
42 Douceur, "The Sybil Attack," 1, 5.
43 Vitalik Buterin and Nathan Schneider, *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains* (Seven Stories Press, 2022), 197–8.

are required to stake … their tokens to present them with a chance of being picked to validate transaction blocks […] The higher the stake, the higher chances a user stands of being chosen".[44]

However, such a mechanism is also vulnerable to third-party interventions, such as the so-called 51% attack.[45] Although PoS might recover after an attack, irrevocably leaked information could damage the inventor's interests and compromise national security interests. Additionally, as PoS derivatives are based on Ethereum, they create risks associated with their origins due to possible connections between Buterin, the mind behind it, and Russian intelligence services.[46]

DPoS is an improved version of the PoS. Reputation is crucial for a network participant to become a sealer.[47] DPoS is the fastest consensus mechanism with the lowest resource consumption. In DPoS each block is created every 3 seconds, compared with PoS – 64 seconds, and PoW – 10 minutes. The reduction in resource consumption is achieved through the centralisation of the block validation process involving witnesses in the system. However, the security risk arises due to the higher degree of centralisation. Witnesses retain their right to create a block for too long, which might be used for malicious activities.[48]

PoW is the computational power-based mechanism. PoW has a reliable mechanism to verify whether the information in the block is valid. Each block, besides containing transaction information, also includes a core feature – the hash – which helps to confirm its validity.

The hash in each block is a compilation of the inherent features of each block, such as a timestamp, a nonce, a reference to the hash of the previous block, and all transactions that occurred before in this chain,[49] as illustrated in Figure 2. The process is dynamic, with the addition of blocks, each time doubling the necessary computational power required to replicate the blocks.

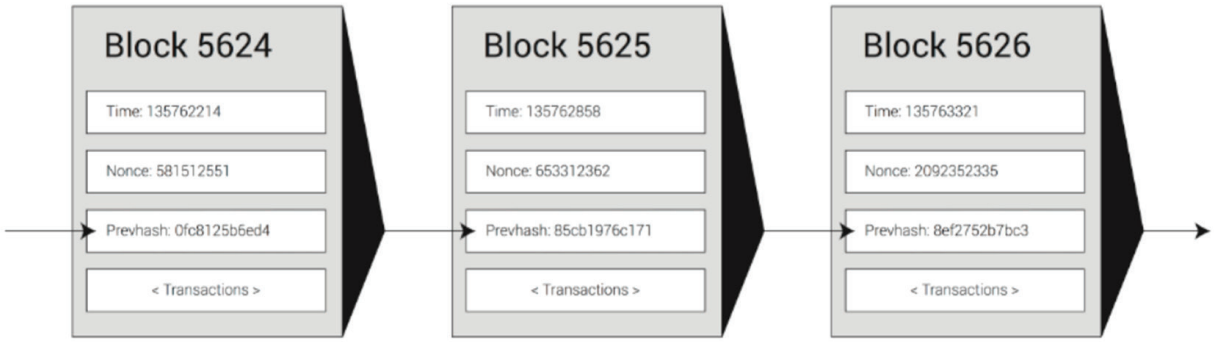

Figure 2. Overview of the blockchain[50]

The following structure allows the creation of a Merkle Tree with block ramification. Each branch has unique hash data, which cannot be altered without changes in the previous blocks. Considering the amount of computational power required to enforce the PoW validation process, it is nearly impossible to compromise the Merkle Tree by replicating all these blocks.[51] At the same time, the development of supercomputers is a key vulnerability that undermines the PoW mechanism. If a single party manages to accumulate more than half of the total hashing power, PoW becomes vulnerable to the 51% attack.

Hybrid approaches allow to combine the strength of different mechanisms, by applying them at distinct validation stages. For instance, node selection may apply the PoW approach, assigning each node a single vote to enhance the decentralisation, while a sophisticated downgrade mechanism, – based on the calculation

---

44 Sheikh Munir Skh Saad and Raja Zahilah Raja Mohd Radzi, "Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS)," *International Journal of Innovative Computing* 10, no. 2 (2020): 28, https://doi.org/10.11113/ijic.v10n2.272.

45 Akbar et al., "Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses," 7.

46 Nathaniel Popper, "Blockchain Will Be Theirs, Russian Spy Boasted at Conference," *The New York Times*, April 29, 2018, https://www.nytimes.com/2018/04/29/technology/blockchain-iso-russian-spies.html.

47 Qian Hua et al., "An Improved Delegated Proof of Stake Consensus Algorithm," *Procedia Computer Science* 187 (2021): 343.

48 Yang et al., "Delegated Proof of Stake with Downgrade," 2–3.

49 Ibid., 7.

50 Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," 6.

51 Akbar et al., "Distributed Hybrid Double-Spending Attack Prevention Mechanism," 6–7.

of node reputation, – can remove malicious nodes from validation process.[52] Although hybrid mechanisms remains untasted, they may offer: "... higher levels of security and performance". [53]

Therefore, the application of hybrid mechanisms should be considered in licensing agreements for dual-use technologies. When designing such a system, criteria including resource consumption, validation speed, vulnerability to different attacks, and the mechanism's capacity to mitigate attacks risks are useful for assessing its efficiency.

The Concepts of the Blockchain Adoption. The article identifies three possible blockchain adoptions: smart contract, blockchain-based SCM and dispute resolution.

Smart contracts are one of the most popular methods for integrating blockchain into the operational life cycle of a licensing agreement. A smart contract is an "if, then" statement, where: "if a condition is met, then a result is executed". From a legal perspective, it is defined through the concept of promises: "…specified in digital form, including protocols within which the parties perform on these promises".[54]

C. Poncibo provides three interpretations of the smart contract definition. Firstly, a smart contract is considered to be "…a computerised transaction protocol that executes the terms of a contract"; secondly it is described as "a self-executing piece of code situated on the shared ledger and maintaining its own state and that is theoretically immutable…"; and lastly, from a legal perspective, it is referred to as "smart (legal) contracts that generally contain the essential elements of a valid and binding contract according to the common standards of domestic contract laws".[55]

In the context of cross-border transactions, smart contracts are considered a key tool for enterprises to revolutionise the management and organisation of their operations "...[s]mart contracts enable the creation of what we call open networked enterprises based on a new set of business models, or old business models with a blockchain twist".[56] Therefore, smart contracts are the basic application of blockchain for risk allocation in cross-border transactions.

Blockchain-based SCM adoption has two fundamental approaches shaping its structure: "(i) planning, implementing, and controlling the primary activities and delivering value for the ultimate customers, and (ii) the integration and coordination of corresponding business processes within as well as across the companies".[57]

The implementation of blockchain into SCM is described as: "… an organised and systematic network between a company and its suppliers to manufacture and sell a particular product to the final customer, aimed at reducing costs and being competitive in the market".[58]

The participants of the supply chain may vary depending on the classification provided. One of the classifications includes entities such as: "suppliers, manufacturer, distributors, retailers, and consumers";[59] another focuses on: "manufacturer, distributor, logistics, and end-users",[60] with an example in Figure 3.

From a technical perspective, blockchain is implemented in blockchain-based SCM systems in two ways: as a smart contract chain between the parties of the supply chain, and as DLT, which consists of all corresponding information about these transactions. The deployment of a smart contract into a blockchain-based SCM makes the process automatic through the: "validating the manufacturer, distributor, logistics, end-users, and terminating the supply chain, using the data recorded in the blockchain".[61]

There are two ideas behind the blockchain-based SCM implementation in licensing agreements. The first is internal – to provide the licensee and licensor with reliable data, enhancing the decision-making process and enabling the precise identification of potential risks for their subsequent allocation between the parties. For such purposes, it is necessary to look at the possible blockchain adoptions more broadly than just the money transfer process.[62] The second is external, which helps to comply with governmental inquiries into transactions' information.[63]

---

52 Yang et al., "Delegated Proof of Stake with Downgrade," 7.
53 Ibid.
54 Deloitte, *Applying Blockchain in Securitization: Opportunities for Reinvention*, Structured Finance Industry Group and Chamber of Digital Commerce, 6, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-sfig-report-applying-blockchain-in-securitization-opportunities-for-reinvention.pdf.
55 Poncibò, "The Digitalization of Contracts in International Trade and Finance," 134–5.
56 Don Tapscott and Alex Tapscott, *Blockchain Revolution*, 36.
57 Aslam et al., "Factors Influencing Blockchain Adoption in Supply Chain Management Practices," 36.
58 Sana Al-Farsi et al., "Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities," *Applied Sciences* 11, no. 12 (2021): 4, https://doi.org/10.3390/app11125585.
59 Ibid., 5.
60 S. Samundeswari et al., "Supply Chain Management of Dual-Use Drugs Using Blockchain," *Procedia Computer Science* 230 (2023): 391.
61 Samundeswari et al., "Supply Chain Management of Dual-Use Drugs Using Blockchain," 391.
62 Rabia Bajwa and Farah Tasnur Meem, "Intellectual Property Blockchain Odyssey: Navigating Challenges and Seizing Opportunities," 7*, arXiv preprint* (2024).
63 Deloitte, *Applying Blockchain in Securitization*, 17.

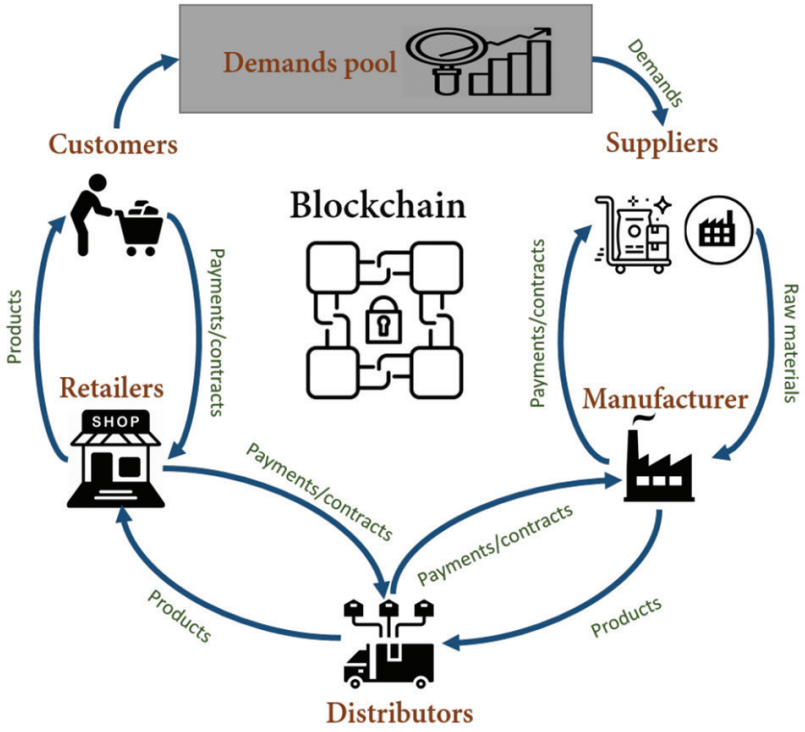

Figure 3. Supply chain participants [64]

Thus, the blockchain-based SCM might be implemented in the supply chain of dual-use technologies in the EU market to enhance data exchange for the purposes of risk allocation in cross-border licensing agreements.

Blockchain-based online dispute resolution (**ODR**) is based on smart contracts' self-enforcement mechanism. It reduces demand for court intervention into commercial disputes, meanwhile the New York Convention enforcement mechanism[65] might be replaced by blockchain-based arbitration platforms.[66]

Firstly, despite the state's authority to enforce legally binding contracts, blockchain technology offers algorithms for the automatic enforcement of parties' obligations. Such a mechanism operates more efficiently than the judicial system:

> Smart contracts make it the case that promisors will do precisely what they promise, radically strengthening promises. If this is the point of judicial contract enforcement, then it looks like smart contracts offer superior technology, and smart contracts would leave judicial enforcement essentially obsolete.[67]

Secondly, blockchain-based platforms and smart contract integrations significantly enhance the efficiency and popularity of ODR. Despite the disadvantages described by the author, ODR has the potential: "to introduce blockchain into the judicial system, having a beneficial impact on the efficiency and accessibility of justice".[68] The outcome of the dispute is self-enforced via the mechanism of smart contract, which neither produces a *res judicata* effect nor provides a classical arbitration award.[69]

The blockchain-based arbitration proceedings, powered by a smart contract self-enforcement mechanism, include the following stages. Initially, participants in the transactions are the holders of so-called digital keys. To enter an obligation, participants use their key to make their promises and store the coin, similar to an escrow mechanism; however, this process is blockchain-based instead of involving an intermediary. The coins under transaction are frozen until the obligation has been performed. After an obligation has been

64 Al-Farsi et al., "Security of Blockchain-Based Supply Chain Management Systems," 5.
65 United Nations, *Convention on the Recognition and Enforcement of Foreign Arbitral Awards*, New York, June 10, 1958.
66 Dincer, "Arbitration in the Age of Blockchain," 99.
67 Kevin Werbach and Nicolas Cornell, "Contracts Ex Machina," *Duke Law Journal* 67, no. 2 (2017): 356.
68 A. Zhuk, "Applying Blockchain to the Modern Legal System: Kleros as a Decentralised Dispute Resolution System," *International Cybersecurity Law Review* 4 (2023): 354, 362, https://doi.org/10.1365/s43439-023-00086-x.
69 Andrea Bonomi et al., eds., *Blockchain and Private International Law* (Brill, 2023), 650.

performed, the performer signals using their digital key. At the same time, the other party may confirm the performance or raise a dispute, holding the coins frozen. To access the coins, both parties ask a private adjudicator, under previously agreed conditions, to resolve the dispute based on gathered evidence in a reliable form. Thus, it constitutes "a form of self-enforcing arbitration, where the issuance of an arbitral decision and its practical implementation… factually overlap entirely".[70]

The number of blockchain-based platforms are suitable for the purpose of dispute resolution arising from smart licensing agreements. For instance: Kleros, empowered by the usage of "game theory and blockchain in a multipurpose dispute resolution protocol",[71] recognised by the EU Commission;[72] Mattereum, which integrates transaction assets and contractual rights into the blockchain with: "...a razor-sharp focus on enforcement"[73]; Jur, which is powering a Network State, that claims to be a "quasi-state"[74], with its own online jurisdiction to settle disputes in the blockchain realm.[75]

Thirdly, the prospect of replacing the New York Convention mechanism with a blockchain-based self-enforcement mechanism is realistic. Although concerns remain regarding raising issues about the perceived legal uncertainty of such an ODR method and the absence of a clear legal framework these considerations are included in the zone of possible development of ODR, and it is a question of time when *lex cryptographia* will overlap conventional dispute resolution.

2. Risk Allocation in Licensing Agreements of Dual-use Technologies at the Intersection of Ukrainian and EU Jurisdictions

Risk in foreign economic activity is defined as: "...the possibility of positive and negative deviations from the predicted desired outcome of decisions related to the integration of a domestic enterprise into the global economy and the implementation of foreign economic agreements".[76] Moreover, risk has a bilateral aspect, where an entrepreneur could either win or lose.[77]

From a legal perspective, the risk relates to the negative aspect of the possible non-performance of a result agreed upon between contractual parties. Legal instruments allow the shifting of risk incidence independently of the parties' actions or intentions after the contract has been concluded.[78] In terms of contractual formation, risk can be allocated between parties by shifting the responsibilities onto the contractual parties in cases where certain circumstances have occurred. The legal mechanisms of risk allocation in licensing agreements are further described in the subsequent sections below.

The concept of risk allocation is described as an inherent tension between parties caused by their attempt: "…to minimize its overall risk and maximize its reward"; at the same time, while seeking to gain benefits from mutual cooperation, the parties define all possible risks together and identify who is responsible for each particular risk and to what extent.[79] This concept in legal and economic literature is also considered one of the methods for "enlarging the contractual pie".[80]

The risk allocation concept is governed by two economic principles used in the exchange of goods. The first is the fundamental theory of exchange, which stipulates that transaction efficiency increases when parties have a comparative cost advantage regarding the goods and services they provide. Applied to risk allocation, this theory suggests that the risk is better shifted to the party best positioned to manage it. The second is the general theory of competitive equilibrium, which asserts that the quantity of goods exchanged is optimal when the marginal costs and benefits of the last unit of goods exchanged are equal for both the provider and the receiver. In the context of risk allocation, this means that risk should be transferred to the party until the marginal costs to the risk bearer are equal to the marginal benefits to the risk shifter.[81]

---

70 Pietro Ortolani, "The Impact of Blockchain Technologies and Smart Contracts on Dispute Resolution: Arbitration and Court Litigation at the Crossroads," *Uniform Law Review* 24, no. 2 (2019): 434–6.

71 Clément Lesaege et al., "Kleros: Long Paper v2.0.2," (2021), 54, https://kleros.io/yellowpaper.pdf.

72 European Commission, Competence Centre on Foresight: Kleros, Knowledge for Policy, July 14, 2020, https://knowledge4policy.ec.europa.eu/foresight/tool/dlt4good/kleros_en.

73 Mattereum, *Mattereum Protocol: Turning Code into Law*, Summary White Paper, February 7, 2020, 2–3, https://mattereum.com/2020/02/07/summary-white-paper/.

74 Balaji Srinivasan, *The Network State: How to Start a New Country* (Kindle edition, 2022), 9.

75 Jun Hong Tan, "Blockchain 'Arbitration' for NFT-Related Disputes," *Contemporary Asia Arbitration Journal* 16, no. 1 (May 2023): 164.

76 Antonina Sviderska, "The Concept and Classification of Risks in Foreign Economic Activities of an Enterprise," *Galician Economic Bulletin* 46, no. 3 (2014): 114, https://galicianvisnyk.tntu.edu.ua/pdf/46/184.pdf [in Ukrainian].

77 Anna Stankiewicz-Mróz et al., *Foreign Economic Activity of Enterprises* (Lodz University of Technology, 2019), 107.

78 Sealy, "Risk in the Law of Sale," 226.

79 *Risk Allocation and Pricing Approaches: Guidance Note*, 4–6.

80 Mirambell Fargas, "Economics of Arbitrability in International IP Contracting," 226.

81 Mauel, "Common Contractual Risk Allocations in International Power Projects," 38.

In a systematic view, risk is manageable within corporate strategies. The strategy for such management includes four stages. The first stage is the identification of risks inherent in a particular type of activity, often achieved through a "risk matrix". The second stage involves risk analysis and evaluation, with special attention given to the likelihood and frequency of risk occurrence. The third stage, which is optional, offers four possible solutions, one of which is risk transfer via a contract. The last stage involves monitoring and managing the implemented strategy to ensure its effectiveness.[82]

Risks Inherent to Cross-Border Licensing Agreements. There are three risks identified in the following subsection: jurisdiction, counterfeiting, and royalty evaluation.

Jurisdiction is a major challenge in cross-border IP transactions, particularly industrial property, that is subject to registration. The challenge is caused by a lack of an international registration system, and by an insufficient international legal framework to protect intellectual property worldwide.[83] There are several mechanisms to register a patent internationally, such as the Patent Cooperation Treaty[84] (**PCT**) and Unitary Patent (**UP**).[85] Although they partially simplify the process, they have significant drawbacks. First, the filing of a patent application under the PCT does not automatically grant the inventor a patent in all States Parties to the treaty but only gives the applicant a 30-month period, as a general rule, to obtain protection in these jurisdictions, according to Article 22(1) of PCT. Secondly, while a UP application provides automatic registration of a patent in all jurisdictions that opt into this mechanism, the number of these jurisdictions is limited, by Articles 3(2) and 7(1) of the EU Regulation No 1257/2012. Therefore, an inventor seeking patent protection for their inventions in different jurisdictions across the globe faces fragmented legal regulations of different legal systems.

To identify risks arising from jurisdictional matters, the following licensing model has been developed, which is divided into registration and licensing stages. The registration stage, as a process of obtaining a European patent by Ukrainian inventors, is described in Figure 4. The process is divided into three steps, where a Ukrainian inventor: 1) registers the patent in Ukraine; 2) applies for international registration under the PCT to the World Intellectual Property Office (**WIPO**); and 3) obtains a European patent under UP in accordance with the relevant guidelines.[86] After completing the registration stage, the licensing of technologies within the EU jurisdiction is possible.

At the licensing stage, jurisdiction risks may arise from the relationships between a inventor and a manufacturer, which is formalised through a licensing agreement, and from possible infringements in the distribution market, as shown in Figure 5.

The application of blockchain for risk allocation is limited in this context, by the exclusive jurisdiction rule. The exclusive jurisdiction rule on intellectual property matters is established under Article 16(4) of the Brussels I Regulation.[87] The rule stipulates that disputes concerning intellectual property rights (**IPR**), including their "subsistence, scope, validity, registration and infringement" might be subject to dispute resolution only in the domestic jurisdictions where the respective IPR were issued. However, decisions, – which do not affect: "the records of the registries of a State, namely inter alia IPRs first ownership and entitlement issues as well as transferability and assignability matters and the contractual transfer of ownership", – may be resolved outside of the respective domestic jurisdiction.[88]

A slightly different principle is established in Article 2:205 of the Principles on Conflict of Laws in Intellectual Property (**CLIP**).[89] Paragraph 2:205.C05 of the Commentary on CLIP states that "a clear distinction must be made between jurisdiction concerning the right to the patent and jurisdiction concerning registration or validity of a registered right".[90] Thus, the exclusive jurisdiction rule does not apply to the issue of patent entitlement, also known as simple ownership disputes, "which must be determined on the basis of the legal relationship which existed between the parties concerned".[91]

---

82 Michael Mills, "Insurance and Risk Solutions for Commercial Products," *Australian Mining & Petroleum Law Journal* 20, no. 1 (2001): 46–7.

83 Reinsch, "E-Commerce: Managing the Legal Risks," 177.

84 Patent Cooperation Treaty 1970.

85 Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, *Official Journal of the European Union* L 361/1 to 8 of 31.12.2012.

86 *Euro-PCT Guide: PCT Procedure at the EPO*, European Patent Office.

87 European Economic Community, *Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, OJ L* 299/32 (entered into force Feb. 1, 1973).

88 Ubertazzi, *Exclusive Jurisdiction in Intellectual Property*, 10.

89 European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Conflict of Laws in Intellectual Property* (Oxford University Press, 2013).

90 Ibid., 121.

91 European Court of Justice, Judgment of the Court (Fourth Chamber) of 15 November 1983, Case 288/82.

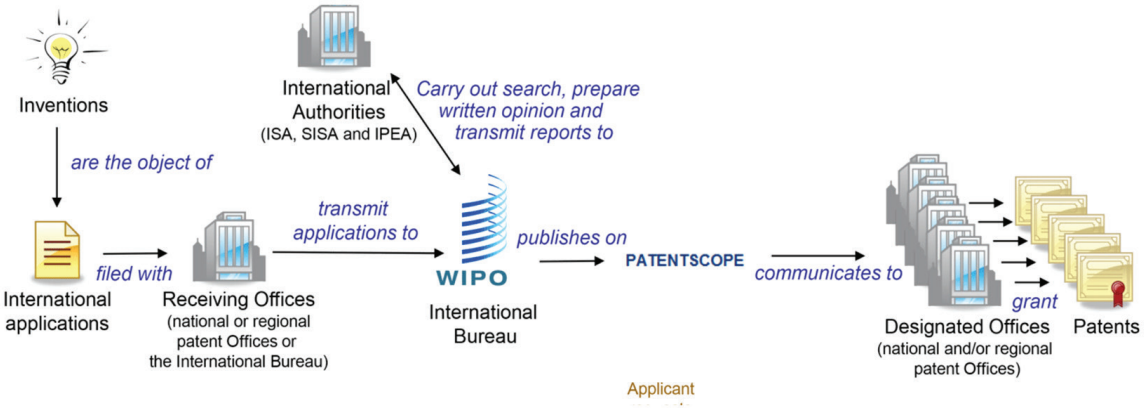

Figure 4. Registration stage [92]

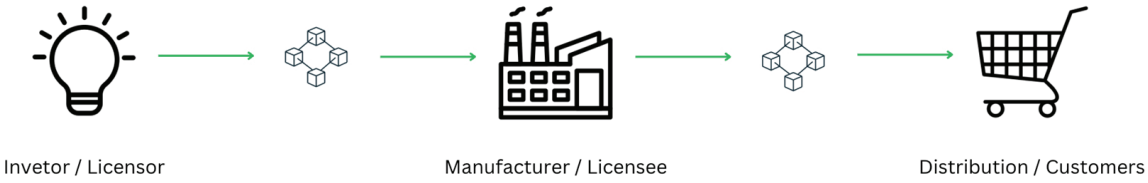

Figure 5. Licensing stages through the blockchain

In addition, differences might arise in the law that governs the licensing agreement and related contractual obligations. The legal framework of the EU patent system is governed by the Regulation on Unitary Patent Protection, which creates an umbrella of unitary patent protection within the "Participating Member State", in the meaning of Article 2(a) of the EU Regulation No 1257/2012. Regarding this regulation and with reference to the provisions of Art. 4(2) of Rome I Regulation[93] and Art. 8(2) of Rome II,[94] there are two types of law governing the obligations arising from the licensing agreement that can be distinguished. First, the contractual obligations arising directly from the licensing agreement are usually "be governed by the law of the country where the licensor is established"; second, the derivative obligations arising from delicts against intellectual property under the respective licensing agreement "are governed by the lex loci delicti".[95]

Thus, for the purposes of this research, it is necessary to divide the jurisdictional risk into two categories: the risk related to interventions into the records of state registries undertaken by the licensor, and the risk that is not governed by the exclusive jurisdiction rule. Nevertheless, the second category must be clearly divided into infringement cases and simple ownership disputes, which are undertaken by the licensee and might be subjected to blockchain risk allocation respectively, as shown in the Table, paragraph 1.

Counterfeiting is a risk in cross-border licensing agreements and might be allocated by the parties through blockchain facilities. Combating counterfeiting and IPR enforcement requires the adoption of a broad approach that goes beyond the licensing agreement itself. In scholarly literature and in practice, blockchain technology adoption for SCM, is a well-known method. It has a preventive character, addressing the roots of counterfeiting,[96] rather than relying solely on "fire extinguishing" measures directed at enforcement bodies or courts.

To combat counterfeiting it is necessary to implement measures which might be categorised into four main categories, including: "internal security, external security, product labelling, and legal safeguards".[97]

---

92 World Intellectual Property Organization, *Protecting your Inventions Abroad: Frequently Asked Questions About the Patent Cooperation Treaty (PCT),* accessed September 11, 2025, https://www.wipo.int/pct/en/faqs/faqs.html.

93 Regulation (EC) No 593/2008 of the European Parliament and of the Council on the law applicable to contractual obligations, 17 June 2008.

94 Regulation (EC) No 864/2007 of the European Parliament and of the Council on the law applicable to non-contractual obligations, 11 July 2007.

95 Kaesling, "The European Patent with Unitary Effect," 94–5.

96 Alzahrani and Bulusu, "Block-supply chain," 35.

97 Felix Engelmann et al., "Intellectual property protection and licensing of 3d print with blockchain technology," in *Transdisciplinary Engineering Methods for Social Innovation of Industry 4.0* (IOS Press, 2018), 104, https://doi.org/10.3233/978-1-61499-898-3-103.

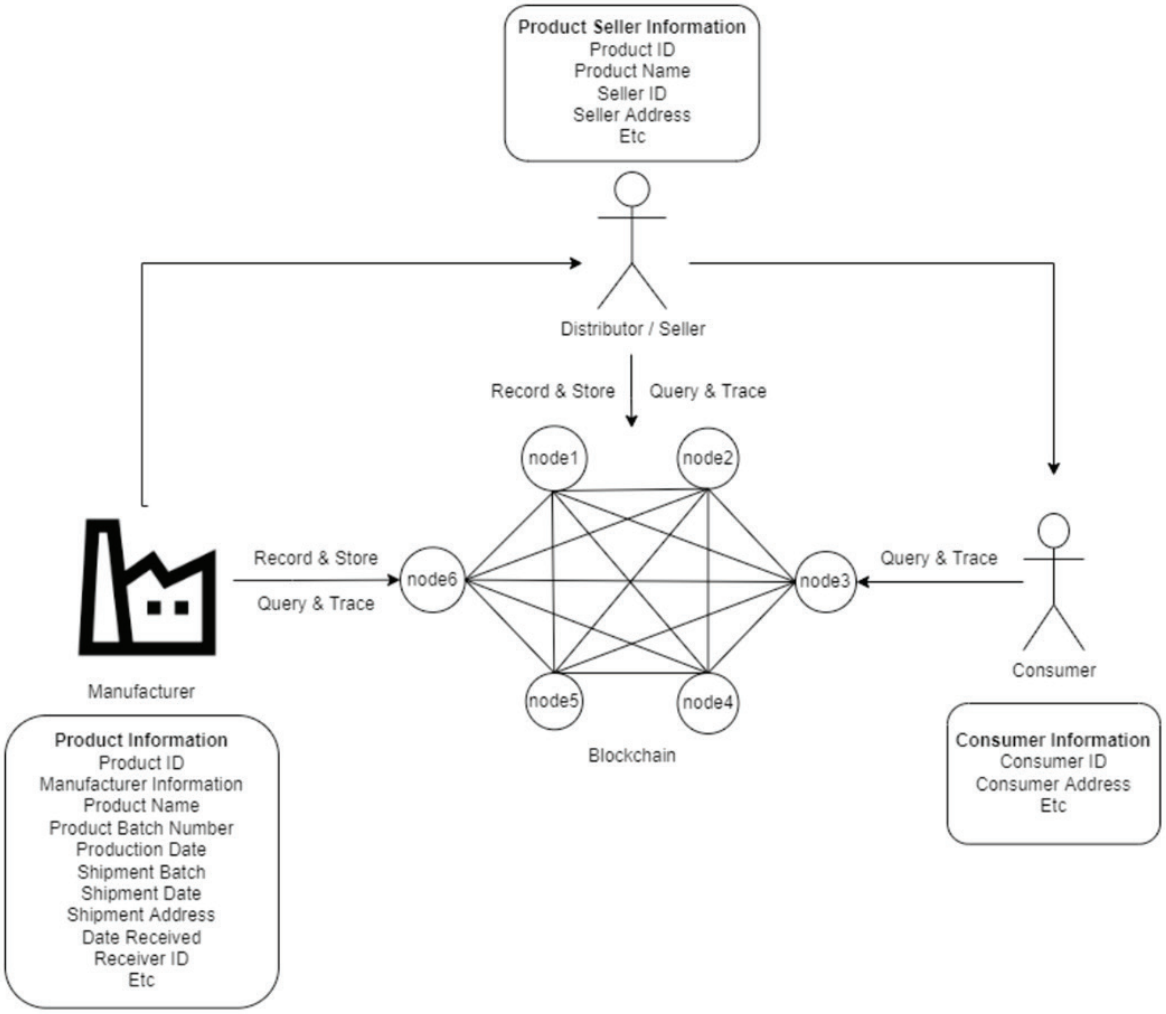

Figure 6. System model diagram [98]

From the perspective of internal security, it is necessary to set up a smart contract chain in distribution, which provides reliable information for buyers of the technologies under licensing agreements. Such information is also applicable for disclosure to "customs officials, to certify a genuine product and tell it apart from a counterfeit".[99]

The implementation of QR codes and/or radio frequency ID for each unit of goods and subsequent registration in the DLT provides each interested party with relevant privileges with access to the information about the tracing and tracking of products, as well as the number of goods sold or in stock in real time. Such a system provides numerous benefits for the licensor and the licensee, including accelerating market demand and conducting market research.[100]

The integration of blockchain-based SCM into the operational cycle of a licensing agreement benefits all participants in the supply chain, including customers, manufacturers, and suppliers, but primarily the licensee and licensor.

The implementation of a smart contract chain to distribute the technology under licensing agreements allows "query and trace the product information and whole transaction history using its product ID; [and] ... span from the manufacturer to the end customer or even resellers… [where] each step of the transaction will be recorded and registered in the blockchain..."[101]

---

98 Michael Christian Lee et al., "Developing an Anti-Counterfeit System Using Blockchain Technology," *Procedia Computer Science* 216 (2023): 89.

99 Jitasha Bahl, "Blockchain and Its Application in the Field of Intellectual Property Rights," *Law Essentials Journal* 2, no. 2 (2021): 306.

100 Gurkaynak et al., "Intellectual Property Law and Practice in the Blockchain Realm," 860.

101 Ibid., 89–90.

In EU jurisdiction the legal solution namely the "anti-counterfeit infrastructure" already exists regarding trademarks and industrial design, which is aimed "to ensure product authenticity throughout the whole supply chain, and eventually beyond".[102] The project developed blockchain-based three-level infrastructure to combat counterfeiting: "Verifiable Credentials (VCs): to format, present, and formalise claims to … IP rights holders. Non-Fungible Tokens (NFTs): to represent the digital twins of products. Blockchain ledger: to create an audit trail and provenance of products".[103]

Another way to combat counterfeiting is the constant review and development of the technologies. The need for the development is a necessity, rather than luxury, especially, considering that in some EU jurisdictions where third parties have access to the practice and improvement of patented inventions.[104] To stay competitive and overturn competitor's attempts to replicate the technology, special attention should be paid to the research and development (**R&D**). The risks of counterfeiting in this context might be allocated through the inventor's efforts in organisational matters. Establishing a transfer project team to enhance permanent communication between the licensor and the licensee is an organisational practice to increase the effectiveness of licensing agreements and R&D facilities.[105]

The last resort of IPR protection is enforcement in the respective jurisdiction where the licensee operates. Such costs "includes the costs for the identification of infringers and litigation costs [...] for enforcement but also defending IPRs".[106] It is advisable to allocate such risk to the licensee, because usually the licensee is in the best position to manage it. The model of counterfeiting risk allocation is shown in the Table, paragraph 2.

The shared royalties model powered by blockchain can avoid informational risks. In scholarly literature fourth types of royalties are commonly distinguished: the first is per-unit royalties, where a fixed amount is paid for each unit of goods sold; the second is ad valorem royalties, calculated as a percentage of revenue from sales[107] (also called profit-sharing royalties), the third type is fixed fees paid for a specified period of time, and the fourth is a mixed types combining features of the above methods.[108]

From an economic perspective, the grounds for selecting one of the possible strategies depend on the licensor's capacity to produce the technology independently. When there is insufficient capacity, the author suggests that it is preferable to choose a fixed fee due to the absence of competition between the licensor and the licensee. However, when the licensor has sufficient capacity to produce and thus compete in the market, the appropriate licensing method in technology is output-based royalties, allowing the licensor some control over the licensee's production volumes.[109] This point becomes controversial in cases where "the patented technology does not drive the demand for the product".[110]

From the perspective of fulfilling obligations to maintain high quality goods and subsequently increasing revenues and royalties, the profit-sharing royalty model appears to be the most efficient. The allocation of these risks promotes cooperation and a shared model of responsibilities, enhancing the potential outcome of the licensing agreement.

At the same time, to generate trust in such relationships, it is necessary to address both information asymmetries: regarding patent value at the licensing agreement conclusion stage, and regarding verification of the criteria for assessing the licensee's effectiveness, at the performance stage.

At the stage of concluding a licensing agreement, the patent owner possesses complete information about the technology in question. From the potential licensee's perspective, there is a risk of insufficient reliable information regarding the potential value, which might be generated by the acquisition of the license. Meanwhile, this lack of transparency can be mitigated through appropriate formation of licensing terms.[111] During the license performance stage, there is a lack of criteria for assessing licensee effectiveness' assessment. To share the risks associated with decline in demand for licensed goods, royalties could be tied

---

102 Eleonora Rosati, "From Web 2 to Web 3: Harnessing Blockchain Technology for IP," Alicante News, EUIPO (2024), https://www.euipo.europa.eu/en/news/from-web-2-to-web-3-harnessing-blockchain-technology-for-ip.

103 European Commission, *EBSI-ELSA (EUIPO): Helping Enterprises, Consumers, and EU Economies at Large Address the Counterfeiting of Products by Increasing Supply Chain Transparency,* European Blockchain Services Infrastructure, accessed September 11, 2025, https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI-ELSA+EUIPO.

104 Toshiko Takenaka, "Patents for Sharing,134, https://doi.org/10.36645/mtlr.26.1.patents.

105 Ene, "Intellectual Property Strategy," 42.

106 Bastidas Venegas, "Intellectual Property Rights, Enforcement Costs and EU Competition Law," i38.

107 Cuihong Fan et al., "Per Unit vs. ad Valorem Royalty Licensing," *Economics Letters* 170 (2018), 2-3.

108 Colombo et al., "Patent Licensing and Capacity in a Cournot Model," 47.

109 Ibid.

110 Llobet et al., "The Optimal Scope of the Royalty Base in Patent Licensing," 3.

111 Bekkers et al., "Overcoming Inefficiencies in Patent Licensing," 3.

to the licensee's net profit. However, an obstacle to implementing this practice is the difficulty in sharing access to the reliable marginal cost information.[112]

Thus, blockchain technology could serve as an instrument for risk allocation during the performance of parties' obligations. The obligation to use this technology could be incorporated into the contract to allocate risks associated with royalty determination by the sharing of reliable information: specifically, information about the patent's value before entering into a licensing agreement; and about the licensee's supply chain and the relative costs associated with its net profit formation, as shown in the Table, paragraph 3.

Risks Inherent in the Field of Dual-Use Technology. There are two subcategories of risk which might be allocated by blockchain-based SCM: export and sanction controls.

Regarding export control, the major concern relates to a lack of transparency in technology transfer through a licensing agreement and the subsequent distribution of those technologies. The principle that may be applied to export rules for dual-use and military technologies is formulated as follows: a government cannot authorise the export of those technologies "unless it can ensure that the export will not harm [its] security".[113]

The established framework for dual-use export control, *inter alia,* including EU Regulation No. 2021/821 provides that Member States' authorities may prohibit the transit of dual-use items where they might be transferred to countries that are subject to an arms embargo.[114]

However, the lack of European jurisdiction and enforcement body control does not prevent the distribution of dual-use and military technologies against EU regulations. The risk associated with "monitoring the production and use of products manufactured using the investor's patented technology" is present,[115] given that each EU Member State has its own approach to legal controls on arms exports, as well as due to the lack of enforcement mechanisms to implement embargoes.[116] This situation may lead to a violation of Ukrainian national interest and security while transferring the technologies abroad.

There are precedents of transferring dual-use and military technologies through the EU border control "to Israel, Morocco, Russia and Venezuela that were approved or supported by Member State governments when there were good reasons under the EU criteria to refuse the deals".[117] Obviously, the situation has changed since the summer of 2014, but to what extent?

The sanctions under EU Council Regulation No. 833/2014 of 31 July 2014 (**EU Regulation No. 833/2014**)[118] introduce a complete ban on the export of dual-use technologies to the Russian Federation. Subsequently, further amendments significantly enhanced the anti-circumvention mechanism and expanded the categories covered under dual-use technologies for the purposes of sanction regulations.[119]

On December 18, 2023, through the twelfth package of sanctions, a new measure on combating sanctions circumvention was introduced. The package amends EU Regulation No. 833/2014 by Art. 12g, which included so-called "no re-export to Russia" measures. These measures impose an obligation on exporters to include a contractual clause prohibiting their counterparties from re-exporting dual-use technologies to the Russian Federation, and mechanisms for imposing a complete ban on export to third countries, which are engaged in circumvention measures.[120] The latest updates on sanctions measures are the 19th package of sanctions, which extended the lists of sanctioned persons, but did not change the methodology.[121]

However, the effectiveness of such measures is limited to the EU jurisdiction. Even though, the EU adopts a more "robust (or 'hard') approach to extraterritoriality in the realm of sanctions… [which] may fall within the realm of permissible collective countermeasures under Article 54 of ARSIWA", – EU sanctions

---

112 Gallini and Wright, "Technology Transfer under Asymmetric Information," 150.

113 Robert A. Borich, "Globalization of the U.S. Defense Industrial Base: Developing Procurement Sources Abroad Through Exporting Advanced Military Technology," *Public Contract Law Journal* 31, no. 4 (2002): 628.

114 Regulation (EU) 2021/821 on a Union regime for the control of exports.

115 Bohdan Pshenychnyi, "International Legal Regulation of the Transfer of Military and Dual-Use Technologies as a Form of Investment," *Ukrainian Journal of International Law* 2 (2024): 30, https://doi.org/10.36952/ujil.2024.2.27-33.

116 Sabatino, "Arms Supplies to Ukraine: Does the European Arms Export Control System Need Revision?," 4.

117 An Vranckx, *Rhetoric or Restraint? Trade in military equipment under the EU transfer control system* (Academia Press, 2010), 3.

118 Council Regulation (EU) No 833/2014 of 31 July 2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine.

119 European Union, *Restrictive Measures in View of the Situation in Belarus and the Involvement of Belarus in the Russian Aggression Against Ukraine. Adopted by the EU under Program BLR*.

120 Council Regulation (EU) 2023/2878 of 18 December 2023 Amending Regulation (EU) No 833/2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine.

121 Council Decision (CFSP) 2025/2032 of 23 October 2025 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

cannot always be effectively applied on an extraterritorial level due to the lack of leverage in bargaining over the trade balance, where "the overall EU economy and the well-being of its population" are at stake.[122]

Hence, it is necessary to consider private sector behaviour and assess the effectiveness of sanctions measures from the perspective of their primary goal – to reduce the military capabilities of the Russian Federation and make its conduct more costly. The sanctions mechanism has become insufficient for reducing export volumes to sanctioned entities due to the options offered by third countries and "their territories to mediate and favour the acquisition of banned products through triangulation and re-exporting activities".[123] Consequently, to allocate the risk of transferring dual-use goods to third countries where their end-use purposes are not verified, the principle of due diligence should include "adequate verification of the customer or partner [and] the intermediaries…"[124]

In this context the use of blockchain provides the parties to the contract with the possibility to allocate such risks. The blockchain SCM facilitates export control, where DLT is key to improving transparency across supply chains.

The research by the Korean Security Agency of Trade and Industry provides three major examples of the implementation of the blockchain-based SCM in dual-use export control. The first is Louis Vuitton's AURA platform that allows the tracking of "the lifecycle of its products, from design and raw materials to manufacturing and distribution […] to track supply chains and streamline compliance processes".[125] The second is a DLT joint project between the government and exporters, which enables merchants to ensure "traceability of sensitive items and support post-shipment verification; […] to validate the identities of their recipients and the authenticity of their end-user documents".[126] The third is "SLAFKA" – a DLT that tracks the nuclear material chain at the national level. SLAFKA "... allows holders of nuclear material to digitally transact between one another while the regulator(s) observe and verify the transactions in near real time".[127]

Thus, implementation of the blockchain-based SCM into the operations of the licensee allows for the allocation of the lack of transparency risk in export and sanctions control for dual-use goods distribution, as shown in the Table, paragraph 4.

Risk Allocation Matrix. The Table "Potential Risks Allocation" presents the possible ways of risk allocation in cross-border transactions associated with licensing agreements of dual-use technologies at the intersection of the Ukrainian and EU jurisdictions. The column "Risks categories" is structured according to the analyses of the present research. In the columns: "Licensor" and "Licensee" the description of risks undertaken by respective parties of the licensing agreement are provided. The last column is "Blockchain application", which represents the risks that might be allocated by blockchain technology.

Table. **Potential Risks Allocation**

No	Risks Categories	Licensor	Licensee	Blockchain application
1	**Jurisdiction**	state register interventions disputes	the infringements of IPR in Licensee's jurisdiction	blockchain-based ODR
2	**Counterfeit**	R&D investment, project teams	IPR enforcement and litigation	anti-counterfeit DLT systems
3	**Royalty Structure**	information asymmetry on royalty base	information asymmetry on patent value	transparent data exchange on profit & supply chain
4	**Export / Sanctions Control**	transfer risks to restricted entities	violation of export and sanction control	blockchain SCM for traceability and end-use checks

Conclusions

Three major risks inherent in cross-border licensing agreements fall into three categories of risks that may be allocated by blockchain technology. The first risk involves disputes arising from various domains established in multiple jurisdictions; such risks may be partially allocated by parties via blockchain-based ODR methods, to a limited extent that does not contradict the exclusive jurisdiction rule. The second is the risk of counterfeiting, which might be mitigated by the mutual efforts of the parties in technological

[122] Silingardi, "The EU 11th and 12th Packages of Sanctions Against Russia," 8–9.
[123] Giumelli, "A Comprehensive Approach to Sanctions Effectiveness," 212, 214–6.
[124] Giorgio Corain, "EU Customs Procedure During the Russo-Ukrainian War: The Prohibitions on the Export of Dual-Use Goods and the Sanctions on Russia," *Università Ca' Foscari Venezia*, 2023/2024, 99.
[125] Vestergaard, "Streamlining Export Controls with Blockchain," 41.
[126] Ibid., 44.
[127] Ibid., 45.

innovation, enhanced enforcement of IPR, and sophisticated blockchain-based anti-counterfeit infrastructure. The third risk related to royalty methods, offers a way to allocate risk of information asymmetry associated with both royalty base formation and the potential value of the patent for the licensee's operations; considering the adoption of a blockchain-based SCM into the operations of both licensor and licensee, they could allocate the risk regarding such asymmetry.

Regarding the control over distribution of dual-use technologies, the lack of transparency in the supply chain is identified as a core risk in such licensing agreements. The presented risks relate to both insufficient export control in the EU jurisdiction and the EU's lack of power to impose extraterritorial sanctions on the transfer of dual-use technologies to the Russian Federation via third countries. At the same time, blockchain developments suggest an effective way to allocate these risks between parties. The results are achieved by tracking respective supply chains and verifying end-use purposes using information contained in a distributed ledger.

Bibliography

Akbar, Nur Arifin, Amgad Muneer, Narmine Elhakim, and Suliman Mohamed Fati. "Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses." *Future Internet* 13, no. 11 (2021): 285. https://doi.org/10.3390/fi13110285.

Al-Farsi, Sana, Muhammad Mazhar Rathore, and Spiros Bakiras. "Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities." *Applied Sciences* 11, no. 12 (2021): 5585. https://doi.org/10.3390/app11125585.

Alzahrani, Naif, and Nirupama Bulusu. "Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain." In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 30–35. 2018. https://doi.org/10.1145/3211933.3211939.

Aslam, Javed, Aqeela Saleem, Nokhaiz Tariq Khan, and Yun Bae Kim. "Factors Influencing Blockchain Adoption in Supply Chain Management Practices: A Study Based on the Oil Industry." *Journal of Innovation & Knowledge* 6, no. 2 (2021): 124–34.

Bahl, Jitasha. "Blockchain and Its Application in the Field of Intellectual Property Rights." *Law Essentials Journal* 2, no. 2 (2021): 302–308.

Bajwa, Rabia, and Farah Tasnur Meem. "Intellectual Property Blockchain Odyssey: Navigating Challenges and Seizing Opportunities." *arXiv preprint* (2024).

Bastidas Venegas, Vladimir. "Intellectual Property Rights, Enforcement Costs and EU Competition Law." *Journal of Antitrust Enforcement* 11, issue supplement_1 (2023): i37–i56. https://doi.org/10.1093/jaenfo/jnac027.

Bekkers, Rudi, Elena M. Tur, Joachim Henkel, Tommy van der Vorst, Menno Driesse, and Jorge L. Contreras. "Overcoming Inefficiencies in Patent Licensing: A Method to Assess Patent Essentiality for Technical Standards." *Research Policy* 51, no. 10 (2022). https://doi.org/10.1016/j.respol.2022.104590.

Bonomi, Andrea, Matthias Lehmann, and Shaheeza Lalani. *Blockchain and Private International Law*. Brill, 2023.

Borich, Robert A. "Globalization of the U.S. Defense Industrial Base: Developing Procurement Sources Abroad Through Exporting Advanced Military Technology." *Public Contract Law Journal* 31, no. 4 (2002): 623–77.

Buterin, Vitalik, and Nathan Schneider. *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains.* Seven Stories Press, 2022.

Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform." *White paper* 3, no. 37 (2014): 2–1.

Colombo, Stefano, Luigi Filippini, and Debapriya Sen. "Patent Licensing and Capacity in a Cournot Model." *Review of Industrial Organization* 62, no. 1 (2023): 45–62.

Corain, Giorgio. "EU Customs Procedure During the Russo-Ukrainian War: The Prohibitions on the Export of Dual-Use Goods and the Sanctions on Russia." *Università Ca' Foscari Venezia*, 2023/2024.

Council Regulation (EU) 2023/2878 of 18 December 2023 Amending Regulation (EU) No 833/2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine. *Official Journal of the European Union, L series*, 2023.

Council Decision (CFSP) 2025/2032 of 23 October 2025 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. *Official Journal of the European Union, L series*, 2025.

Council Regulation (EU) No 833/2014 of 31 July 2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine. *OJ L* 229 (2014): 1–11.

De Filippi, Primavera, and Aaron Wright. *Blockchain and the Law: The Rule of Code.* Harvard University Press, 2018.

Deloitte. *Applying Blockchain in Securitization: Opportunities for Reinvention*. Structured Finance Industry Group and Chamber of Digital Commerce. Accessed September 11, 2025. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-sfig-report-applying-blockchain-in-securitization-opportunities-for-reinvention.pdf.

Dincer, Yigit Efe. "Arbitration in the Age of Blockchain." Master's thesis, Université de Montréal, 2023.

Douceur, J. R. "The Sybil Attack." In *Lecture Notes in Computer Science*, edited by P. Druschel, F. Kaashoek, and A. Rowstron. Vol. 2429. Springer, 2002.

Ekparinya, Parinya, Vincent Gramoli, and Guillaume Jourjon. "The Attack of the Clones Against Proof-of-Authority." arXiv preprint arXiv:1902.10244 (2019).

Ene, Sebastian-Ioan. "Intellectual Property Strategy – With main focus on patents and licensing of patents." Master's thesis, NTNU, 2014.

Engelmann, Felix, Martin Holland, Christopher Nigischer, and Josip Stjepandić. "Intellectual property protection and licensing of 3d print with blockchain technology." In *Transdisciplinary Engineering Methods for Social Innovation of Industry 4.0,* 103–112. IOS Press, 2018. https://doi.org/10.3233/978-1-61499-898-3-103.

European Commission. "Competence Centre on Foresight: Kleros." Knowledge for Policy, July 14, (2020). Accessed September 11, 2025. https://knowledge4policy.ec.europa.eu/foresight/tool/dlt4good/kleros_en.

European Commission. "EBSI-ELSA (EUIPO): Helping Enterprises, Consumers, and EU Economies at Large Address the Counterfeiting of Products by Increasing Supply Chain Transparency." European Blockchain Services Infrastructure. Accessed September 11, 2025. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI-ELSA+EUIPO.

European Court of Justice. Judgment of the Court (Fourth Chamber) of 15 November 1983. *European Court Reports,* Case 288/82 (1983).

European Economic Community. *Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters*. *OJ L* 299/32 (entered into force Feb. 1, 1973).

European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP). *Conflict of Laws in Intellectual Property*. Oxford University Press, 2013.

European Patent Office. "*Euro-PCT Guide": PCT Procedure at the EPO.* 16-th edition. Munich, 2023. Accessed September 11, 2025. https://link.epo.org/web/legal/guide-europct/en-euro-pct-guide-2023.pdf.

European Union. Restrictive Measures in View of the Situation in Belarus and the Involvement of Belarus in the Russian Aggression Against Ukraine. Adopted by the EU under Program BLR. Accessed September 11, 2025. https://www.sanctionsmap.eu/api/v1/pdf/regime?id[]=2&lang=en.

Fan, Cuihong, Byoung Heon Jun, and Elmar G. Wolfstetter. "Per unit vs. ad valorem royalty licensing." *Economics Letters* 170 (2018): 71–5.

Gallini, Nancy T., and Brian D. Wright. "Technology Transfer under Asymmetric Information." *The RAND Journal of Economics* 21, no. 1 (1990): 147–60.

Giumelli, Francesco. "A Comprehensive Approach to Sanctions Effectiveness: Lessons Learned from Sanctions on Russia." *European Journal on Criminal Policy and Research* 30, no. 2 (2024): 211–28.

Gurkaynak, Gonenc, Ilay Yilmaz, Burak Yeşilaltay, and Berk Bengi. "Intellectual Property Law and Practice in the Blockchain Realm." *Computer Law & Security Review* 34, no. 4 (2018): 847–62.

Hua, Qian, Biwei Yan, Yubing Han, and Jigou Yu. "An Improved Delegated Proof of Stake Consensus Algorithm." *Procedia Computer Science* 187 (2021).

Joshi, Shashank. "Feasibility of proof of authority as a consensus protocol model." arXiv preprint arXiv:2109.02480 (2021).

Kaesling, Katharina. "The European Patent with Unitary Effect – A Unitary Patent Protection for a Unitary Market?." *UCL Journal of Law and Jurisprudence* 2 (2013): 87–111.

Lashkari, Bahareh, and Petr Musilek. "A Comprehensive Review of Blockchain Consensus Mechanisms." *IEEE Access* 9 (2021): 43620–52.

Lee, Michael Christian, Rafaelle Richel Pearl, Ivan Sebastian Edbert, and Derwin Suhartono. "Developing an Anti-Counterfeit System Using Blockchain Technology." *Procedia Computer Science* 216 (2023): 86–95.

Lesaege, Clément, William George, and Federico Ast. "Kleros. Long Paper. v2.0.2." (2021). Accessed September 11, 2025. https://kleros.io/yellowpaper.pdf.

Llobet, Gerard, and Jorge Padilla. "The Optimal Scope of the Royalty Base in Patent Licensing." *Chicago Journals* 51, no. 1 (2014).

Mattereum. "Mattereum Protocol: Turning Code into Law." Summary White Paper, February 7, 2020. Accessed September 11, 2025. https://mattereum.com/2020/02/07/summary-white-paper/.

Mauel, John G. "Common Contractual Risk Allocations in International Power Projects." *Columbia Business Law Review* 1996, no. 1 (1996): 37–60.

Mills, Michael. "Insurance and Risk Solutions for Commercial Products." *Australian Mining & Petroleum Law Journal* 20, no. 1 (2001): 46–64.

Mirambell Fargas, Miquel dels Sants. "Economics of Arbitrability in International IP Contracting." *Journal of Law and Commerce* 37, no. 2 (2019): 179–264. https://doi.org/10.5195/jlc.2019.164.

Ortolani, Pietro. "The Impact of Blockchain Technologies and Smart Contracts on Dispute Resolution: Arbitration and Court Litigation at the Crossroads." *Uniform Law Review* 24, no. 2 (2019): 430–48.

Patent Cooperation Treaty, 1970, 28.7 U.S.T. 7645, T.I.A.S. No. 8733.

Poncibò, C. "The Digitalization of Contracts in International Trade and Finance: Comparative Law Perspectives on Smart Contracts." In *Digitalization and Firm Performance*, 131–55. Springer International Publishing, 2022.

Popper, Nathaniel. "Blockchain Will Be Theirs, Russian Spy Boasted at Conference." *The New York Times*, April 29, 2018. Accessed September 11, 2025. https://www.nytimes.com/2018/04/29/technology/blockchain-iso-russian-spies.html.

Pshenychnyi, Bohdan. "International Legal Regulation of the Transfer of Military and Dual-Use Technologies as a Form of Investment." *Ukrainian Journal of International Law* 2 (2024): 27–33. https://doi.org/10.36952/ujil.2024.2.27-33.

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), 2008. *OJ* L 177/6.

Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). *OJ* L 2007, 199/4001.

Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection. *Official Journal of the European Union* L 361/1 to 8 of 31.12.2012.

Reinsch, Roger. "E-Commerce: Managing the Legal Risks." *Managerial Law* 47, no. 1/2 (2005): 168–96.

Risk Allocation and Pricing Approaches: Guidance Note, prepared by Government Commercial Function. London: GCF, 2021. Accessed September 11, 2025. https://assets.publishing.service.gov.uk/media/60a388a9e90e07357baa83da/Risk_allocation_and_pricing_approaches_guidance_note_May_2021.pdf.

Rosati, Eleonora. "From Web 2 to Web 3: Harnessing Blockchain Technology for IP." Alicante News, EUIPO (2024). Accessed September 11, 2025. https://www.euipo.europa.eu/en/news/from-web-2-to-web-3-harnessing-blockchain-technology-for-ip.

Sabatino, Ester. "Arms Supplies to Ukraine: Does the European Arms Export Control System Need Revision?" *EU Non-Proliferation and Disarmament Consortium* 89 (2024).

Samundeswari, S., V. Lalitha, V. Kavitha, M. Harini, T. Dharshini, and S. Srinithi. "Supply Chain Management of Dual-Use Drugs Using Blockchain." *Procedia Computer Science* 230 (2023): 388–97.

Sealy, L. S. "Risk in the Law of Sale." *Cambridge Law Journal* 31, no. 1 (1972): 225–47.

Shiddiq, Naufal Ahmad, Danrivanto Budhijanto, and Mursal Maulana. "The Future of Commercial Arbitration: Blockchain." *Journal of Law, Policy and Globalization* 140 (2024): 40–48. https://doi.org/10.7176/JLPG/140-05.

Silingardi, Stefano. "The EU 11th and 12th Packages of Sanctions Against Russia: How Far is the EU Willing to Go Extraterritorially?" *Global Trade and Customs Journal* 19, no. 7/8 (2024).

Skh Saad, Sheikh Munir, and Raja Zahilah Raja Mohd Radzi. "Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS)." *International Journal of Innovative Computing* 10, no. 2 (2020): 27–32. https://doi.org/10.11113/ijic.v10n2.272.

Srinivasan, Balaji. *The Network State: How to Start a New Country*. Kindle edition. 2022.

Stankiewicz-Mróz, Anna, Viktor Perederii, Valentyna Novak, Oksana Ilienko, Oksana Kyrylenko, Ganna Gurina, Kateryna Razumova, Elvira Danilova, Svitlana Petrovska, and Larysa Lytvynenko. *Foreign economic activity of enterprises*. Lodz University of Technology, 2019.

Sviderska, Antonina. "The Concept and Classification of Risks in Foreign Economic Activities of an Enterprise." *Galician Economic Bulletin* 46, no. 3 (2014): 113–21. https://galicianvisnyk.tntu.edu.ua/pdf/46/184.pdf [in Ukrainian].

Takenaka, Toshiko. "Patents for Sharing." *Michigan Technology Law Review* 26, no. 1 (2019). https://doi.org/10.36645/mtlr.26.1.patents.

Tan, Jun Hong. "Blockchain 'Arbitration' for NFT-Related Disputes." *Contemporary Asia Arbitration Journal* 16, no. 1 (May 2023): 145-[ii].

Tapscott, Don, and Alex Tapscott. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. New York: Portfolio / Penguin, 2016.

Ubertazzi, Benedetta. *Exclusive Jurisdiction in Intellectual Property.* Tübingen: Mohr Siebeck, 2012.
United Nations. *Convention on the Recognition and Enforcement of Foreign Arbitral Awards.* New York, June 10, 1958, 330 U.N.T.S. 3.
Vestergaard, Cindy. "Streamlining Export Controls with Blockchain (블록체인을 통한 수출통제의 효율화)." Professional Report. Stimson Center, Korean Security Agency of Trade and Industry (무역안보 저널). *Trade & Security* 1 (June 2021): 38–50.
Vranckx, An. *Rhetoric or Restraint? Trade in military equipment under the EU transfer control system.* Academia Press, 2010.
Werbach, Kevin, and Nicolas Cornell. "Contracts Ex Machina." *Duke Law Journal* 67, no. 2 (2017): 313–82.
World Intellectual Property Organization. "Protecting your Inventions Abroad: Frequently Asked Questions About the Patent Cooperation Treaty (PCT)". Accessed September 11, 2025. https://www.wipo.int/pct/en/faqs/faqs.html.
Yang, Fan, Wei Zhou, Qingqing Wu, Rui Long, Neal N. Xiong, and Meiqi Zhou. "Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism." *IEEE Access* (2019). https://doi.org/10.1109/ACCESS.2019.2935149.
Zhuk, A. "Applying Blockchain to the Modern Legal System: Kleros as a Decentralised Dispute Resolution System." *International Cybersecurity Law Review* 4 (2023): 351–64. https://doi.org/10.1365/s43439-023-00086-x.

Любов Логуш
Кандидат юридичних наук, доцент
Національний університет «Києво-Могилянська академія», Київ, Україна
https://orcid.org/0000-0003-4753-1768
l.logush@ukma.edu.ua

Максим Баришов
Студент 2 року навчання магістерської програми «Право»
Національний університет «Києво-Могилянська академія», Київ, Україна
https://orcid.org/0009-0003-8562-2326
maksym.baryshov@ukma.edu.ua

РОЗПОДІЛ РИЗИКІВ У ЛІЦЕНЗІЙНИХ ДОГОВОРАХ НА ОСНОВІ БЛОКЧЕЙНУ ЩОДО ТЕХНОЛОГІЙ ПОДВІЙНОГО ПРИЗНАЧЕННЯ НА ПЕРЕТИНІ ЮРИСДИКЦІЙ УКРАЇНИ ТА ЄС

У статті досліджено застосування технології блокчейн для розподілу ризиків у транскордонних ліцензійних договорах щодо технологій подвійного призначення, з урахуванням правового регулювання України та ЄС.

Проаналізовано технологію блокчейн як із технічного, так і з юридичного погляду. Окреслено принципи функціонування найбільш поширених консенсусних механізмів, які застосовуються в управлінні ланцюгами постачання, визначено основні загрози, притаманні кожному з них. Проаналізовано найпоширеніші типи атак проти блокчейн-інфраструктури. Визначено критерії придатності консенсусних механізмів для транзакцій щодо технологій подвійного призначення. Серед можливих способів імплементації блокчейну в ліцензійні договори наведено смартконтракт, управління ланцюгами постачання та врегулювання спорів. Розглянуто впровадження смартконтрактів у ліцензійних договорах в операційний цикл комерційних структур. Наведено можливі підходи до впровадження блокчейну в управління ланцюгами постачання. Описано сучасні методи врегулювання спорів у цифровій сфері.

Також розглянуто впровадження технології блокчейн для розподілу ризиків за транскордонним ліцензійним договором на перетині юрисдикцій України та ЄС. Визначено поняття ризику та його розподілу між сторонами договірних відносин з погляду економіки та права. Виокремлено дві категорії ризиків: притаманні ліцензійним договорам та специфічні для галузі технологій подвійного

призначення. Перша категорія стосується ризиків, пов'язаних із питаннями колізійного права, підробки та формування роялті. Межі розподілу ризиків на основі блокчейну виявляються з огляду на правило виключної юрисдикції. Впровадження управління ланцюгами постачання на основі блокчейну досліджено крізь призму розподілу ризику підробки. Аналогічний підхід застосовано до ризику асиметрії інформації. Друга категорія ризиків стосується експортного контролю та санкцій. Розглянуто нормативно-правову базу ЄС, що регулює відповідні сфери. Проаналізовано сучасні приклади впровадження управління ланцюгами постачання, що використовуються для розподілу ризиків експортного контролю та санкцій. Обидва ризики можуть бути розподілені між договірними сторонами за допомогою управління ланцюгами постачання на основі блокчейну.

Результатом дослідження є формування матриці розподілу ризиків з використанням технології блокчейн.

Ключові слова: блокчейн, розподіл ризиків, транскордонні транзакції, ліцензійний договір, технології подвійного призначення.

Матеріал надійшов 12.09.2025
Схвалено до публікації 12.12.2025
Оприлюднено 31.12.2025