The blockchain ecosystem in the light of intellectual property law

by **Eleni Tzoulia***

Abstract: The study at hand delves into the technologies composing blockchain and designates its most significant practical applications to date. The technological ecosystem identified through this investigation is then scrutinized from the perspective of intellectual property law. It examines, in particular, under which conditions and to what extent blockchain itself as a standalone product, its individual components, and its several applications may be subject to a) copyright, b) database and trade secret protection, and c) patent law. The objective of this investigation is to identify the most suitable legal basis for raising claims against unauthorized use of the pertinent subject matter. The analysis also explores adversities posed to intellectual property law by modern technologies and contemplates their circumvention. The benchmark for this examination is the intellectual property law currently in force in the EU.

Keywords: digital timestamp; smart contract; blockchain database; crypto-patent; know-how

Recommended citation: Eleni Tzoulia, The blockchain ecosystem in the light of intellectual property law 13 (2022) JIPITEC 290 para 1

A. Blockchain's concept and operation

1 "Blockchain" is a type of distributed ledger technology (DLT). It is based on a decentralized Peer-to-Peer (P2P) network, i.e., a set of interconnected computers ("nodes") communicating directly with each other without any central server intervention. Within such networks users share computational resources and content, thus activating a common digital data repository. A particularity of blockchain is that peer nodes cannot interfere with the distributed content, e.g., amend or delete it. The following sections present the technological context behind this feature and comment upon its practical implications.

I. The pertinent technological context

2 Data in blockchain are grouped in blocks, placed one after the other in chronological order, thus forming a chain (as the name "blockchain" indicates). This chain is distributed as a single file to all nodes and each copy is updated on every new data entry. To safeguard the integrity and confidentiality of the entries, blockchain deploys cryptographic algorithms, in particular hash functions and asymmetric (public and private) key encryption.

3 In more detail, before being stored in the blockchain the submitted data get timestamped and converted into bit arrays of fixed length ("digest") by hashing algorithms. The hash output is unique for each

given input and gets adjusted to even the slightest modifications of the latter. In the blockchain pattern, moreover, hash outputs follow a sequential order from block to block. Therefore, any attempt to manipulate data stored in the blockchain shall cause inconsistencies in the hash values between the linked blocks, thus being promptly detected and invalidated.

4 The above hashing process cannot be reversed, i.e., it is not possible to recover the initial content through the corresponding hash value. To this end, a decryption process has to take place which is based on a pair of cryptographic keys. Asymmetric cryptography safeguards secure confidential correspondence between nodes. Namely, although one may anonymously join the network, the exchange of data is permitted only between trusted parties sharing the matching key-pair to lock and unlock the transmitted message.

5 According to the above, data entries in the blockchain are public but secured, in the sense that they are accessible and traceable by all connected nodes but their content can be disclosed only to authorized parties. They also acquire certified content and dates without the mediation of an outer authority or a central administrator. Therefore, it is argued that blockchain seeks "building trust with disintermediation"[1], thus constituting an appropriate tool for the digitalization of transactions that in the analog world would be subject to notarial certification, publicity formalities, and other security mechanisms under the auspices of accredited bodies.

II. Overview of the major blockchain applications

6 The simulation of "trusted surveillance and audit", which is achieved by technological means within the blockchain ecosystem, justifies the fact that the first applications based on this technology referred to "cryptocurrencies", the conclusion and execution of the so-called "smart contracts", as well as the registration and management of digital files potentially subject to intellectual property rights (IPRs). Nevertheless, blockchain is considered to have a much broader scope of application being able to provide new prospects in sectors such as healthcare[2], supply chain tracking[3], elections[4], machine learning[5], etc.

1. Cryptocurrencies

7 The first practical blockchain application has been a digital payment and value transfer system using as currency unit the so called "bitcoin". The code of this system was released in 2008 under the signature of some "Satoshi Nakamoto", a presumed pseudonymous person or team of persons remaining unidentified to date. In the context of this application, blockchain entries relate to bitcoin transactions[6] and may refer to the amount provided each time, its remitter, and the beneficiary.

8 The strong investment interest prompted by bitcoin, incited the release of competitive products with a similar function, thus establishing a category of digital value units characterized as "cryptocurrencies". This term indicates the use of encryption techniques for ensuring the validity and confidentiality of the relevant transactions. The value attributed to cryptocurrencies depends on the competition developed in the relevant market and the forces of supply and demand. Also, the production costs for each type

* Adjunct lecturer for commercial law, Aristotle University of Thessaloniki (AUTH), post-doctoral researcher for law and technology, Hellenic Open University (HOU), Greek State Scholarship Foundation (IKY) Scholar. Email: elena.tzoulia@gmail.com. This paper has been partly produced within the framework of an Austrian Standards Fellowship at the Faculty of Law of the University of Graz.

1 See European Parliament Resolution of 3 October 2018 on Distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), (2020/C 011/03), OJ C 11, 13.1.2020, p 7–14.

2 Blockchain can host e.g. distributed patient data files, which get updated in real-time through wearables and are remotely accessible to all stakeholders (doctors, hospitals and diagnostic centers), thus facilitating telemedicine operations (smart health). See EPO, Patents and the Fourth Industrial Revolution. The inventions behind digital transformation, December 2017, p 74.

3 Traceability of goods, control of counterfeits. See European Parliament Resolution (n 1) rec. 16.

4 See on the "smart voting" issue <https://businesstech.co.za/news/it-services/237547/a-secure-online-voting-system-using-blockchain/> accessed 15 May 2022.

5 It is argued that blockchain can ensure transparency and clarity in the operation of smart software governed by machine learning algorithms which are used in automated decision-making systems. See. Kritikos, European Parliament Scientific Foresight Unit (STOA), What if blockchain could guarantee ethical AI?, PE 656.334, 2020, <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/656334/EPRS_ATA(2020)656334_EN.pdf> accessed 15 May 2022.

6 Such as purchases, sales, and payments.

of cryptocurrency, in terms of computational resources and energy consumption, are of relevance in this respect[7].

9 From a technological perspective, cryptocurrencies are data produced, exchanged, and stored through special software in the decentralized P2P network where blockchain is hosted as described above[8]. This very nature of cryptocurrencies as digital content facilitates the creation and release of unbacked copies which are devoid of any value. To prevent incidences of duplicated cryptocurrencies being used multiple times by the same user[9], peer nodes enforce "consensus protocols". The latter term refers to agreements as to how transactions submitted in the network shall be authenticated by the nodes themselves.

10 To date, the most popular protocols have been the ones known as "proof-of-work" and "proof-of-stake". In their context, nodes compete against each other to compute whether each documented transaction fits in the flow of hash values between the linked blocks.[10] The node solving the puzzle is rewarded with cryptocurrencies. Because this process entails making profits through the expenditure of computational resources and energy, it is also called "mining". Respectively, users engaging in the verification process are called "miners".[11]

2. Smart contracts

11 The term "smart contract" pertains to software programmed to execute particular tasks when certain predetermined conditions are satisfied. Consequently, it does not refer literally to contracts concluded and executed in the digital environment. The program's code rather enforces a consensus that has already taken place in the physical world.[12] For example, an agreement may dictate that in case of a flight delay of X hours, the passenger's account shall be credited with a certain amount of money. In this case, the smart contract software shall automatically launch the compensation process as soon as it receives a delay notice. In this context, blockchain is used as a storage medium for automated transactions, also safeguarding their immutability and confidentiality. Yet, for smart contracts to operate several technologies may need to be deployed, like artificial intelligence (AI), internet of things (IoT), crypto-assets, etc.[13]

12 In the above vein, nowadays self-executable statutes may facilitate the operation of digital associations/partnerships.[14] This is the case with Decentralized Autonomous Organizations (DAOs) which use the "Ethereum" blockchain for the conclusion and execution of the (smart) corporate agreement governing them. In this case, namely, the underlying software allows the establishment and operation of a digital entity resembling a legal person.[15]

3. Digital files timestamping

13 Digital files are inherently susceptible to unauthorized use and counterfeit. To certify the production date of their data and safeguard their integrity, individuals nowadays may use blockchain-based timestamping services administered by Trusted Third Parties (TTP). By being stored in the blockchain the file leaves a unique digital fingerprint, which certifies its existence at a given time and its origin from an identifiable entity. It also becomes tamper-proof and can be traced. The relevant service applies regardless of the digital file's nature as the subject matter of IPRs, i.e., whether it represents a literary, scientific, or artistic "work", an industrial design, a

7 See on the legal nature and the function of cryptocurrencies Chiara Zilioli, 'Crypto-assets: Legal Characterisation and Challenges under Private Law' [2020] E.L. Rev. 251, 266.

8 Christian Engelhardt and Sascha Klein, 'Bitcoins – Geschäfte mit Geld, das keines ist - Technische Grundlagen und zivilrechtliche Betrachtung' [2014] MMR 355 ff.

9 What is known as the "double spending issue".

10 See Daniel Kälberer, 'Blockchain-Technologie: Virtuelle Währungen aus handels- und steuerbilanzieller Sicht' [2021] BC 417, 419 ff.

11 See Matthias Terlau in Herbert Schimansky and others (eds), Bankrechts-Handbuch (5th edn, C.H.Beck 2017) paras 135-140.

12 See Thomas Söbbing, 'Smart Contracts und Blockchain-Technologie. Definition, Arbeitsweise, Rechtsfragen' [2018] ITRB 43; Andreas Börding and others, 'Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht. Praxis und Rechtsdogmatik' [2017] CR 134.

13 Martin Fries, 'Schadensersatz ex machina' [2019] NJW 901, 902 ff.

14 See Shen Wei, 'When FinTech meets corporate governance: opportunities and challenges of using blockchain and artificial intelligence in corporate optimization', [2021] J.I.B.L.R. 53; Gaspare Dori, 'Blockchain, smart contracts and mergers and acquisitions: or how to re-establish trust' [2021] I.B.L.J. 289.

15 See Maximilian Mann, 'Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp? Gesellschaftsrechtliche und kollisionsrechtliche Implikationen' [2017] NZG 1014.

trademark, trade secret, etc. However, timestamping produces evidence of priority and authorship which may be used in the context of related legal disputes. Thus, the future establishment of IPRs on the timestamped file's content may ultimately be facilitated[16].

B. Intellectual property rights on the blockchain-related subject matter

14 Evidently, a blockchain-related industry has currently emerged which hosts various activities, alongside any cryptocurrency transaction and conversion services. Entrepreneurship within the blockchain ecosystem may prove particularly profitable.[17] This potential reinforces the interest of blockchain developers and investors to protect their products against counterfeiting and unauthorized use. To this end, they need to establish exclusive ownership of these assets, enforceable against any competing undertakings. In this and the following section, the study scrutinizes EU intellectual property law as a tool to achieve the above objectives.

15 The complexity and versatility of blockchain poses normative challenges, which in the IP domain in particular manifest themselves in the form of intersections and conflicts between individual IPRs. Indeed, according to the preceding analysis, blockchain constitutes a network of peer nodes which hosts records of encrypted data administered by special software. At the same time, blockchain is a business model apt for digitalizing and decentralizing several legal acts and relationships. Each of these aspects is subject to an individual set of IPRs, which serve distinct purposes and may ensure a different level of protection in each given case. It is questionable, which sector of intellectual property law may provide the broadest and most rounded protection to the blockchain-related subject matter, as well as whether any confluent rights may be exercised conjunctively or the establishment of one right excludes the evocation of the other.

16 Primarily, however, the assumption itself that IP law is in principle applicable within the blockchain ecosystem, is negotiable. The developer of bitcoin, the first known blockchain application to date, published incognito the pertinent code in a whitepaper of 2008. "Nakamoto" continued to edit this code until 2010 and then resigned, thus allowing the free exploitation of the application by third parties. It can therefore be argued that the technologies under consideration have been dedicated to the public domain ever since, thus not being subject anymore to exclusive IPRs.

I. Blockchain-related technologies in the public domain

17 Public domain refers to material which may be used by any person without permission.[18] In the sphere of IP, the public domain comprises products of human intellect that no longer are or have never been subject to private ownership.[19] This status may be in principle attributed to limitations and exceptions of IP law. It is disputed whether the relinquishment of one's own IPRs may effectively place the subject matter concerned within the public domain. Most jurisdictions answer this question in the negative. However, unconditional licensing in the form, e.g., of free and open-source software (FOSS) and the creative commons zero (CC0) licenses, ultimately unfolds the legal effects of IP relinquishment.[20]

1. IP public domain in the EU

18 In EU law in particular, public domain dedication of IP is not regulated concretely. Industrial property law prescribes similar rights, e.g., to formally surrender one's trademarks[21], abandon patents[22], and judi-

16 See also Michèle Finck and Valentina Moscon, 'Copyright law on Blockchains: Between new forms of rights administration and digital rights management 2.0' [2019] IIC 77; Tania Kern, 'Blockchain and intellectual property rights: blockchain anchoring, a ground-breaking means of proof to the rescue of creators?', [2021] I.B.L.J. 279.

17 See for instance the case of "Coinbase", a US company engaging in the intermediation of cryptocurrency transactions <https://www.cbinsights.com/research/report/coinbase-strategy-teardown/> accessed 15 May 2022.

18 Ilanah Simon Fhima, 'The public domain' [2019] I.P.Q. 1.

19 See on the definition and the ratio of public domain in the field of intellectual property Séverine Dusollier, 'The public domain in intellectual property: Beyond the metaphor of a domain' in PL Jayanthi Reddy (ed.), *Intellectual Property and Public Domain* (Icfai University Press Hyderabad 2009) 31.

20 See Graham Greenleaf and David Lindsay, *Public Rights* (Cambridge University Press 2018) 509 ff.

21 See Art. 57 Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trademark, OJ L 154, 16.6.2017, p 1–99.

22 See Art. 87 EPC in conjunction with Rules 45 par. 3 and 162 par. 4 of Implementing Regulations, as well as Guidelines for Examination Part A, Chapter III, par. 5.2, Part B, Chapter III, par. 3.4, Part C, Chapter IX, 1.3.

cially revoke one's IPRs in case of disuse.[23] In all these cases, however, the subject matter concerned does not become communal, but rather subject to exclusive priority IPRs established by third parties. On the other hand, industrial property law and copyright alike, do not provide for the ex officio prosecution of infringements. Therefore, right-holders who waive their claims against violators of their IPRs, legitimize de facto the unauthorized use. Such tolerance, however, cannot be construed as an implicit transfer of one's IP. To this end, a written agreement or an explicit statement is required.[24] What is more, moral rights are regarded as in principle indispensable.

19 In any case, materials incorporating public domain elements may be eligible for IP protection, as long as they demonstrate, for instance, originality from the perspective of copyright, inventiveness from the perspective of patent law, etc.[25] However, the applicable IPRs do not extend to the public domain elements themselves, which shall remain available for everyone to use. In the same vein, intellectual achievements culminating from unauthorized exploitation of third-party IPRs may be eligible for IP protection. As long as the aggrieved parties refrain from raising claims against the violator, the latter can freely and exclusively exploit the secondary product comprising the non-proprietary materials.

2. Framing the blockchain-related public domain

20 According to the above, whether the bitcoin system code has been dedicated to the public domain or not, is not uniformly regulated among legal orders worldwide. The fact is that over the last decade the blockchain ecosystem has significantly evolved. Expert contributions have enriched it with new or improved technologies and new blockchain applications have been devised. No right-holder opposition has been ever expressed against this progress and no IP claims have been raised. Therefore, it appears that the person or team behind the code of bitcoin has unconditionally abandoned any relevant IPRs.

21 Consequently, it could be argued that—either legally or de facto—this primary blockchain application is encompassed by the public domain. However, ownership and individual protection of improvements thereto, as well as novel blockchain-related products and services, may be claimed. This is true, despite the fact that these achievements take advantage of the fundamental blockchain technology and concept. As a result, the abovementioned contemplations on the appropriate legal basis for IP protection must be further examined.

II. Copyright protection for blockchain-related software

22 With regards to software, which constitutes an essential blockchain component, copyright is applicable in principle. This derives in particular from Article 10 paragraph 1 of the TRIPS Agreement, as well as Article 4 WIPO Copyright Treaty (WCT), pursuant to which computer programs are subject to copyright as "literary works" within the meaning of Article 2 of the Berne Convention. These provisions have influenced software protection at an international level. In the EU in particular, the protection of electronic programs is assigned to copyright pursuant to Directive 2009/24/EC.[26]

23 Both Article 9(2) TRIPs and Article 2 WCT provide that copyright protection applies to expressions and not to ideas, procedures, operation methods or mathematical concepts as such. The ratio behind these exceptions relates to not monopolizing ideas, to the detriment of technological progress and industrial development. Accordingly, the object of the protection conferred by Directive 2009/24/EC is the expression in any form of computer programs, as well as the preparatory design material capable of leading to the reproduction or subsequent creation of a program.[27]

24 Computer programs are considered to be expressed through their source and object code.[28] Source code is the algorithm that guides the operation of the program once it is encoded in a programming language. An object code is described as the source code of the program, after being compiled in binary machine language, so that it can be executed by the computer hardware. Preparatory design work may

23 See Art. 58 Regulation (EU) 2017/1001.

24 See Art. 20 par. 3 Regulation (EU) 2017/1001; Art. 8 par. 1 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, OJ L 361, 31.12.2012, p 1–8.

25 See Art. 14 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p 92–125.

26 Directive 2009/24/EK of the European Parliament and Council of the 23rd of April 2009 for the legal protection of computer programs, OJ L 111, 5.5.2009, p 16–22.

27 See article 1 par. 2 and recital 11 of the Directive 2009/24/EC.

28 See article 10 par. 1 TRIPS.

include, for example, structures or organizational charts developed by the programmer, which may be re-transcribed in source code and object code and culminate in the execution of the program.[29] On the contrary, any element comprising ideas and principles or not enabling the program's reproduction directly or indirectly, e.g., the underlying logic and algorithms, any programming languages, the format of data files used to exploit certain functions of the computer program, the graphic interface enabling users to access the program's features[30], as well as the functionality of a computer program are not subject to copyright.[31]

25 According to Article 1 paragraph 3 Directive 2009/24/EC, software in the above sense shall be protected by copyright if it is "original". Originality is regarded as an intrinsic feature of any "work" and copyright protection is in principle reserved for intellectual creations reflecting their author's individuality. In the case of software, however, the relevant threshold is arguably low. In principle, copyright may be acknowledged for any computer program provided that it is not a copy or absolutely banal.[32]

26 In view of the above, it appears that all computer programs in the blockchain ecosystem may be subject to copyright, as long as they do not copy existing software. The protection covers the program's code before and after its compilation, as well as any preparatory design material, but neither the outcome of the program's execution, nor the underlying concept.[33] Consequently, any competitor may reproduce the program's functionality by observing, studying, and testing its operation. The competing product shall not infringe the author's copyright on the model software as long as it relies on a different code. This is true, even if it uses the same programming language and data files. Therefore, it may be argued that copyright promises limited protection for blockchain-related software, so that alternative, or complementary legal bases of IP protection should be explored.

III. The legal framework for database protection and its relevance for blockchain

27 Data records constitute another fundamental feature of blockchain. Compilations of data or other material that by reason of the selection or arrangement of their contents constitute intellectual creations, are subject to copyright. This approach is prescribed on an international level by Article 10 paragraph 2 TRIPS, Article 5 WCT, and Article 2 paragraph 5 of the Bern Convention. It has been also espoused by the EU legislator as apparent from Article 3 Directive 96/9/EC.[34] The latter act complements copyright protection by prescribing a sui generis IP right of EU-limited application scope for "databases".

1. The Directive 96/9/EEC

28 The term database in Directive 96/9/EEC refers to any collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.[35] An independent material is supposed to demonstrate autonomous informative value in relation to the rest database content.[36] Moreover, database materials are systematically or methodically arranged when they are classified according to predetermined criteria, e.g., alphabetically, numerically, etc., rather than randomly accumulated.[37] A database in the above sense is also expected to include technical or other means allowing access to and retrieval of its separate materials.[38]

29 See recital 7 of Directive 2009/24/EC and Opinion of AG Bot in C-393/09 of 14.10.2010, Bezpečnostní softwarová asociace, ECLI:EU:C:2010:611, rec. 63.

30 C-393/09 of 22.12.2010, Bezpečnostní softwarová asociace, ECLI:EU:C:2010:816, rec. 37-42.

31 C-406/10 of 02.05.2012, SAS Institute, ECLI:EU:C:2012:259, rec. 29-46.

32 See Gernot Schulze, 'Geschützte Werke' in Thomas Dreier and Gernot Schultze (Eds) *Urheberrechtsgesetz* (C.H.Beck 2022) 113; Martin Vogel, '§ 87a' in Ulrich Loewenheim and others (Eds) *Urheberrecht (UrhG, KUG, VGG) Kommentar* (C.H.Beck 2020) 1470 ff. Differing view from Marie-Christine Janssens, 'The software Directive' in Irini Stamatoudi and Paul Torremans (Eds) *EU Copyright law: A commentary* (Edward Elgar Cheltenham UK, Northampton MA USA 2021) 75.

33 C-406/10 of the 02.05.2012, SAS Institute Inc., ECLI:EU:C:2012:259, rec. 39-41.

34 Directive 96/9/EEC of the European Parliament and Council, of the 11th of March 1996 on the legal protection of databases , OJ L 77, 27.3.1996, p 20–28.

35 See Art. 1 para 2 Directive 96/9/EEC.

36 C-444/02 of 09.11.2004, Fixtures Marketing v OPAP, ECLI:EU:C:2004:697, rec. 33.

37 Vogel (n 32) 1940.

38 Such as electronic, electromagnetic or electro-optical processes, indexes, tables of contents, etc. See rec. 13

29 Similar to computer programs, databases are eligible for copyright protection provided that they are original, i.e., "the author's own intellectual creation".[39] Copyright covers the selection and arrangement of the database's particles and does not extend to the content itself.[40] Other criteria than that of originality, e.g., aesthetic, or quantitative standards, shall not be applied when determining the eligibility of a database for copyright protection. The originality criterion is satisfied in this case when, through the selection or arrangement of the data, the author expresses their creative ability by making free and creative choices, thus stamping a personal touch.[41] Reversely, the originality criterion is not satisfied when the setting up of the database is dictated by technical considerations, rules or constraints that leave no room for creative freedom.[42]

30 The originality benchmark may discourage ventures into modern information storage and processing systems. To circumvent this risk, in view of establishing a common information market[43], Article 7 et seq Directive 96/9/EEC prescribes a sui generis intellectual property right for the maker of a database where the obtaining, verification, or presentation of the database's contents demonstrates substantial investment in qualitative or quantitative terms. Hence, for this special kind of protection to be granted, it is decisive whether the database maker has dispensed human[44], financial[45], or technical resources[46] to find and collect the database contents, control their consistency and accuracy, classify them, and manage their individual accessibility system.[47] The substantial character of the investment is examined quantitatively, i.e., in relation to its scale, or qualitatively, i.e., in relation to its manner and impact.[48] For instance, an innovative arrangement of the collected materials may represent a considerable investment in human capital in qualitative terms.[49]

31 As long as these conditions are met, the database maker can forbid the extraction and re-utilization in total or to a substantial extent of the database contents by third parties without previous authorization. This is true, irrespective of the commercial purpose of such practices.[50] Namely, a substantial infringement in this case may not only derive from the manufacture of a parasitical competing product, but also from any other use which may cause significant detriment—in quantitative or qualitative terms—to the investment made to set up the database.[51]

32 As it follows from Article 7 in conjunction with Recital 41 of the Directive, the above right is granted to the database "maker". The latter term refers to the person who takes the initiative and bears the risk of investing in the database manufacture. Thus, the auxiliary person who performs the technical work of constructing the database as a simple representative of the person in charge, does not fall under this concept. In other respects, the database maker may equally be a natural or a legal person. More entities bearing the relevant capacity become joint owners and the relationship between them is governed by the applicable national law.[52]

33 The abovementioned right can be transferred, assigned, or granted with or without consideration under a contractual license. It may be established on any database in which either the manufacturer or the rightsholder is an EU national or has at least usual residence within the Union.[53] Copyright and a sui generis IP right can coexist on the same database.[54]

Directive 96/9/EEC and C-444/02 (n 36), rec. 30.

39 See Art. 3 para 1 and rec. 16 of Directive 96/9/EEC.

40 See rec. 26-27 Directive 96/9/EEC.

41 C-604/10 of 01.03.2012, Football Dataco Ltd and others v Yahoo! UK Ltd and others, ECLI:EU:C:2012:115, rec. 38; C-145/10 of 01.12.2011, Painer, ECLI:EU:C:2011:798, rec. 89, 92.

42 C-604/10, ibid, rec. 39; C-403/08 and C-429/08 of 04.10.2011, Football Association Premier League and Others, ECLI:EU:C:2011:631, rec. 98.

43 See rec. 9-12 Directive 96/9/EEC.

44 Man-hours, cognitive energy and expertise, etc.

45 Money in the form of, e.g., funds, salaries, expenses.

46 Equipment, infrastructure, etc.

47 See C-338/02 of 09.11.2004, Svenska Spel, ECLI:EU:C:2004:696, rec. 24-27.

48 See recital 19 Directive 96/9/EEC and C-304/07 of 09.10.2008, Direct media Publishing GmbH, ECLI:EU:C:2008:552, rec. 24; C-203/02 of 09.11.2004, British Horseracing Board, ECLI:EU:C:2004:695, rec. 69 et seq; C-444/02, ibid, rec. 44.

49 Vogel, (n 32) p 1954.

50 C-545/07 of 05.03.2009, Apis-Hristovich EOOD, ECLI:EU:C:2009:132, rec. 40 et seq; C-304/07, (n 48) rec. 29 et seq; C-203/02, (n 48) rec. 46-51.

51 See recital 42 Directive 96/9/EEC.

52 Justine Pila and Paul Torremans, *European Intellectual Property law* (Oxford University Press 2016) 513.

53 See Article 7 par. 3 and 11 Directive 96/9/EEC.

54 Article 7 par. 4 Directive 96/9/EEC.

2. The blockchain database

34 It is argued that the distributed ledger of blockchain represents a database within the meaning of Article 1(2) Directive 96/9/EEC.[55] This is correct in principle, given that the blockchain hosts a collection of data classified in blocks according to their chronological order and technical compatibility. Data entries may be conceptually independent and self-sufficient, irrespective of their intersection and correlation, as is the case with entries referring to individual cryptocurrency transactions, pieces of digital content, diagnostic test results, etc. There is also a particular mechanism in place for nodes retrieving and inspecting each entry separately, i.e., public-key encryption.[56]

35 The database established within the blockchain is potentially subject to copyright, to the extent that the selection and/or arrangement of its content is original. It can be argued that arranging data into blocks, as an inherent and distinguishing feature of blockchain, falls within the realm of the public domain. In any case, separating data in blocks is not a creative arrangement, in particular if it is performed in chronological order and justified by technical reasonings.[57]

36 As far as the sui generis right of Article 7 et seq Directive 96/9/EEC is concerned, it may be conceived as protecting blockchain in its capacity as a carrier medium for the data collection recorded within it.[58] The pertinent protection extends to any technology used for accessing the individual contents of a blockchain database, e.g., decryption keys.[59] From this perspective, all peer nodes in the relevant network shall be regarded in principle as the makers and joint owners of the blockchain database.

37 In this context, no substantial investment can be substantiated with respect to "obtaining" the contents of the blockchain database, since the contents are created rather than sought and found by the nodes. This however does not negate the sui generis protection of Article 7 et seq, as long as the "verification and presentation" of the database contents, i.e., the process of classifying them, verifying, and maintaining their integrity requires high expenditures in computing power, time, and expertise.[60] In public blockchain applications, such as cryptocurrency networks, the "substantial" investment requirement should be deemed fulfilled by only large investors and miners. Thereby, the expanding circle of potential sui generis protection co-beneficiaries shall be restricted, thus also making the exercise of the pertinent rights manageable.[61]

IV. Blockchain and trade secrets law

38 The regulatory framework for trade secrets is commonly retrieved for the protection of subject matter not covered by other IPRs, like algorithms[62], mathematical concepts, and business methods, as well as datasets ineligible for either copyright or database protection.[63] Any piece of information which is not widely known, nor directly accessible to persons operating in the relevant trading sector may be considered a trade secret. Such information is expected to have acquired commercial value precisely because of its secret character and its rightful owner must make reasonable efforts to keep it confidential.[64]

39 The rightful owner enjoys the right to prohibit any unauthorized acquisition, use or disclosure of their trade secrets.[65] However, this does not imply the establishment of an absolute right on protected information. Therefore, the independent acquisition or development of the same know-how, e.g., through research and analysis, or even reverse engineering,

55 Sebastian Pech, 'Who owns the Blockchain? How copyright law allows rights holders to control Blockchains' [2021] J. Bus. & Tech. L. 59, 69 ff.

56 Compare C-444/02, ibid, rec. 28-32.

57 Pech, (n 55) 71.

58 Vogel (32) 1945.

59 See rec. 20 Directive 96/9/EEC.

60 See C-46/02 of 09.11.2004, Fixtures Marketing Ltd v Oy Veikkaus Ab, ECLI:EU:C:2004:694, rec. 34-40; C-203/02, (n 48) rec. 31-36; C-338/02, (n 47) rec. 24-30.

61 See also the relevant contemplations of Pech (n 55) 72 ff.

62 See Katharina Scheja, 'Schutz von Algorithmen in Big Data Anwendungen – Wie Unternehmen aufgrund der Umsetzung der Geschäftsgeheimnis-Richtlinie ihre Algorithmen wie auch Datenbestände besser schützen könne' [2018] CR 485, 487 ff.

63 The legal framework under examination is considered for instance appropriate for the protection of training datasets serving machine learning purposes. See BGH of 28.01.2014, VI ZR 156/13, BGHZ 200, p 38-51.

64 See Article 39 TRIPS and 2 para 1 of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of know-how and business information which has not been disclosed (trade secret) from illicit acquisition, use and their disclosure, OJ L 157, 15.6.2016, p 1–18.

65 See Article 4 Directive (EU) 2016/943.

remains possible.[66] Moreover, non-disclosed innovations are not considered to be a part of "the state of the art" in the pertinent technological field, i.e., knowledge already conquered, that would render any future equivalent achievements "non-novel". As a result, third parties acting in good faith may acquire priority IP rights on the subject matter protected as a trade secret.[67] In any event, the protection of information as a trade secret is considered a restrictive factor on its commercialization.

40 According to the above, the various blockchain-related technologies and applications may be subject to the legal framework for trade secrets, both regarding their technical features and in terms of their character as business schemes. This presupposes, however, that whoever lawfully controls the relevant information takes reasonable steps to safeguard its confidentiality.[68] Distributed ledgers in the narrow sense of the term, like blockchain hosting cryptocurrency transactions, are decentralized P2P networks open for everyone to join by downloading the necessary software for free and entering into the pertinent consensus protocol. The legal protection prescribed for trade secrets is extraneous to the public character of such applications. On the contrary, private blockchain networks, e.g., smart contracting, smart health, timestamping applications, etc., that allow a limited number of persons — commonly whoever has been granted a license — to connect, could be protected as trade secrets.[69] This presupposes, however, that all interconnected nodes are bound by a confidentiality agreement.

V. The shift towards patent law

41 Patents are legal titles establishing IPRs on inventions. Competent authorities grant them after having scrutinized the claimed subject matter with regards to its novelty and inventiveness, i.e., its contribution to the state of the art. Patent law provides protection for entire technological achievements, as individual products delivering certain tangible outcomes. Therefore, in comparison to copyright, patents can extend the protection granted by IP law beyond the source/object code to the functionality of a program. From another perspective, patent granting presupposes the disclosure of all details related to the implementation of the claimed invention. As a result, it is supposed to contribute to the dissemination of knowledge and the enhancement of innovation by simultaneously circumventing any competitive risks associated with the confidential character of know-how.

42 In view of the aforementioned advantages, patent law is increasingly being invoked as a legal basis for protecting blockchain-related technologies and applications. However, the capacity of achievements from the IT sector to be patented is subject to certain limitations on an international level.[70] In the following section the study analyses the requirements for patenting blockchain-related subject matter, pursuant to the provisions in force within the European legal order.

C. Blockchain-related subject matter in the light of patent law

43 Patent granting is in principle administered by provisions of national reach. Accordingly, the rights deriving from a patent are territorial, in the sense that the protection granted covers the national territory where the examination authority is based. International treaties have nonetheless established unified procedures for granting patents of broader scope.

44 Such a treaty is the European Patent Convention (EPC). Based on the pertinent legal framework, an undertaking may make patents enforceable in all member states of the EPC through one single application and examination process.[71] More specifically, European patents are enforceable in all EU member states and several third countries.[72]

66 See Article 3 and recital 16 Directive (EU) 2016/943.

67 Anthoula Papadopoulou, 'Creativity in crisis: are the creations of artificial intelligence worth protecting?' [2021] jipitec 408, 416.

68 See Thomas Söbbing, 'Schutz von Algorithmen. Rechtliche Anforderungen und vertragliche Gestaltung' [2019] ITRB 192, 194.

69 Christian Hess, 'Die Blockchaintechnologie im Lichte des Geschäftsgeheimnisschutz- und Patentrechts' [2020] GRUR-Prax 251.

70 See for the United States Antonio DiNizo, 'From Alice to Bob: The patent eligibility of blockchain in a post-CLS Bank world' [2018] Journal of Law, Technology & the Internet <https://scholarlycommons.law.case.edu/jolti/vol9/iss1/2>.

71 These are not patents automatically valid in all Member States of the Convention, such as those regulated by Regulation (EU) 1257/2012 of the European Parliament and of the Council of 17.12.2012 establishing enhanced cooperation in the field of establishing a single patent protection regime, OJ L 361, 31.12.2012, pp 1-8.

72 European patents are also recognized in certain candidate countries for EU accession and in third countries (validation states).

The examination of European Patent applications is carried out by the European Patent Office (EPO). The EPO's Boards of Appeal are competent on a supranational level to revoke European patents.

I. Software and database patentability pursuant to the EPC

45 EPC does not define the term "invention" but includes a non-exhaustive list of non-inventions in Article 52 paragraph 2. Accordingly, mathematical methods, business practices, information presentations and computer programs fall foul of the invention concept, thus being in principle patent-ineligible. However, pursuant to paragraph 3 of the same Article, this is true inasmuch as a patent application refers to the excluded subject matter "as such".

46 Thus, even though achievements from the IT sector appear to be explicitly excluded from patent law protection, it is ultimately acknowledged that EPC makes their patentability conditional upon the demonstration of "technical character". Indeed, Article 27 of the TRIPS Agreement defines inventions as "products or processes, in all fields of technology", thus implicitly declaring that patent law protection is meant for creations from the technical field. This postulation was not explicitly adopted in the EPC until its amendment in 2000.[73] However, its implicit embrace has always been apparent from the repeated references to the technical realm in the provisions of the Convention itself, as well as in the implementing regulations, and the examination guidelines that complement and specify it.

47 Whether an invention from the IT sector demonstrates a technical character is examined on a case-by-case basis, in light of the EPO's "two-hurdle" approach.[74] In this context, a two-stage examination is carried out. First, it is examined whether the claimed subject matter exploits technical means or is rather confined to theoretical considerations. Accordingly, any subject matter invoking the use of hardware, e.g., an electronic device, for its operation or implementation may be patented, even if it falls in principle under the list of Article 52 paragraph 2 EPC.[75]

48 Subsequently, an examination whether the claimed invention solves a technical problem by the claimed technical means must be conducted. The invention will be ultimately deemed patentable, if it solves the technical problem in a novel way that is not obvious to the average person skilled in the art. A technical solution is in principle effectuated by software that, e.g., controls the operation of a machine or an industrial process. However, when it comes to the software controlling only the internal functions of a computer without tangible results in the external world, as is the case for the so-called system[76], application[77], and network[78] software, as well as for various kinds of utility programs[79], a "further technical effect" must be demonstrated.

49 Accordingly, the required technical character is not evident from the mere activation and operation of a computer by means of the program.[80] In this respect, it is also not sufficient that the program merely automates a process from the analog environment. On the contrary, a patentable program is expected to dictate a new structure for the computer system or a new way of functioning by adding new features or fixing malfunctions.[81]

50 Therefore, methods of processing, classifying, analyzing, distributing, etc., digital data cannot be pat-

73 See OJ EPO 2007, Special Edition 4, p 48. Accessible via: http://archive.epo.org/epo/pubs/oj007/08_07/special_edition_4_epc_2000_synoptic.pdf.

74 T 0641/00 (Two identities/COMVIK) of 26.9.2002.

75 This formula is known as "any hardware approach", having been outlined in the context of the decision T 0931/95 of 8.9.2000 (Controlling pension benefits system) and consolidated by the decision T 0258/03 of 21.4.2004 (Auction method/HITACHI). See also T 0424/03 (Clipboard formats I/ MICROSOFT) of 23.2.2006. Accordingly, it has been found sufficient that a patent application invokes, e.g., the use of a computer or a computer-readable storage medium (CD, DVD) or a smart card or an electronic communication network, etc., to successfully pass the first stage of the examination process.

76 System software manages a computer's main resources, i.e., central processing unit (CPU), memory, disk drivers, etc., and its peripherals. It mainly consists of operating systems (OS).

77 Application software refers to programs directing a computer to execute specific tasks according to the user's commands. It includes word processors, web browsers, music players, etc.

78 This software category encompasses applications facilitating the establishment and operation of networks and data sharing among electronic devices.

79 This term refers to software support, maintenance, and development tools and comprises programs like compilers, linkers, debuggers, etc.

80 T 1173/97, Computer program product/IBM, of 01.07.1998, rec. 6 et seq

81 See T 0172/03 (*Order management/RICOH*) of 27.11.2003; BGH X ZB 23/74 (*Dispositionsprogramm*) of 22.06.1976; T 1784/06 (*Classification method/COMPTEL*) of 21.09.2012.

ented, to the extent that the technical effect they generate is confined to the execution of business or administrative practices and other mental processes by technical means.[82] Any effects achieved through automation relating, e.g., to the acceleration of procedures, saving energy and time, etc., are not regarded as technical solutions. Similarly, the presentation of digital data by means of software and electronic devices does not demonstrate in principle any technical character. The fact that such presentations may achieve a more accurate or enjoyable communication of information to the user, does not constitute a solution to any technical problem.[83]

II. The blockchain patentability in the European patent system

51 Given that blockchain is based on a decentralized computer network, any blockchain-related subject matter may fall within the concept of a Computer-Implemented Invention (CIIs) in the light of the EPC. Its patentability is therefore governed by the above rules, being conditional in principle upon consolidating its technical character.[84] To this end, one must prove that the claimed invention in each given case brings about a further technical effect, i.e., a technical solution through technical means.

52 As evident from the preceding analysis, the various blockchain applications automate in principle procedures and practices from the analog environment. This is true not only for smart health, smart voting, smart contracting systems, etc. Also, the cryptocurrency blockchains simulate in essence the financial system. The idea of decentralizing monetary transactions by substituting any auditing authorities for technological safeguards and mutual consent, constitutes a business model. Such applications do not establish the technical character required for being patented.[85]

53 Nevertheless, several technological achievements within the blockchain ecosystem could successfully claim patent protection. These may relate, e.g., to software for preventing malicious attacks and data leaks, securing the accessibility, consistency, and confidentiality of data entries in the network, etc. The EPO in particular has examined applications for encryption technologies[86], data timestamping[87], etc. In the United States, where software patentability requirements resemble the ones in force within the European patent system[88], patents have been granted for, inter alia, blockchain verification technologies[89], systems for transforming traditional domain names into blockchain user addresses[90], etc.

D. Concluding remarks

54 Nowadays, humanity is experiencing the fourth industrial revolution that is arguably distinguished by the convergence of the natural, biological, and digital environment. Many technological developments confirm this observation, such as principally the rise of artificial intelligence, the internet of things and the digitalization of the economy. The latter circumstance relates roughly to the dematerialization of transactions and the emergence of new economic activities taking place exclusively online. The implementation of the contemporary digital economy has been largely facilitated by blockchain, whose im-

82 This is the case, e.g., for order management systems, T 0172/03 of 27.11.2003, (*Order management/RICOH*); supply chain management applications, BGH X ZB 23/74 of 22.06.1976, (*Dispositionsprogramm*); data analysis serving billing and scoring purposes, T 1784/06 of 21.09.2012 *(Classification method/ COMPTEL)*, etc.

83 It is exceptionally conceivable that a technical problem is solved by a presentation of information. Such an effect has been attributed for instance to a method making it easier for the user to search and select images stored on an electronic device by displaying them in low resolution and in a side-by-side order on the screen. T 0643/00 (Searching image data / CANON) of 16.10.2003. Technical character is also stipulated in relation to presentations of information that are intended to guide the user in performing technical tasks or to function as electronic signals of the conditions prevailing within a computer system. T 1741/08 (GUI layout/SAP) of 2.8.2012, para 3.3; T 0336/14 (Presentation of operating instructions/GAMBRO) of 2.9.2015; T 1802/13 (Brain stimulation/CLEVELAND) of 10.11.2016; T 2084/18 (Suspicious behavior/AIC) of 18.6.2021, para 3.2.

84 Hess (n 69) 253.

85 See T 0994/18 (Secure mobile payment/ADVANCED NEW TECHNOLOGIES) of 20.7.2021: The invention consisting in a distributed networked system exchanging encrypted and unencrypted data does not demonstrate any technical character, as long as it relates to a payment system, thus to a business method.

86 T 2327/17 (Authenticated encryption of audio data/BOSCH) of 21.2.2020; T 0556/14 (Masking a private key/CERTICOM) of 28.7.2016.

87 T 1408/09 (Group identifier/SQUARE ENIX) of 7.9.2017.

88 DiNizo (n 70).

89 Shlomit Yanisky-Ravid and Edward Kim, 'Patenting blockchain: Mitigating the patent infringement war' [2019/2020] Albany Law Review 603, 613, footnote 54.

90 US Patent No. 10,721,060 of 21.07.2020, Verisign INC.

plications have incited investments in the field, thus also spotlighting the issue of the IP law relevance for protecting any blockchain-related subject matter.

55 It is not self-evident that blockchain technologies and applications may be subject to IP rights. It has been argued that the code of bitcoin may be regarded as part of the public domain. This assumption, however, does not negate IP protection per se for achievements that develop the primary technological context and/or introduce new practical uses of blockchain. On the contrary, their pertinent eligibility shall be examined in light of the general rules of IP law.

56 What rights exactly could a business active in the blockchain ecosystem protect and on which legal basis, is an issue requiring scrutiny and meticulous justification. The preceding analysis has revealed that concepts and methods being implemented by means of blockchain, like smart contracting, can only be protected as trade secrets. This presupposes however their confidentiality, which for many reasons may be undesirable in business practice.

57 Even though blockchain functionalities do not fit easily in the IP domain, individual technologies supporting the blockchain operation, as well as the database formed within it may be subject to a wide spectrum of IPRs. Even though the conditions for their establishment differ significantly and shall be examined on a case-by-case basis, the concurrent rights may overlap on the same subject matter. In that case they may be cumulatively invoked by the right-holder, unless certain limitations posed, e.g., their duration, or any conflicts of interest, advocate for the one in lieu of the other. For instance, the confidentiality prescribed for trade secret protection and the "sufficient disclosure" requirement of patent law contradict with each other. Also, the identification of the IP right-holder may prove challenging with respect to DLTs, where all nodes contribute to the creation and arrangement of the distributed content. Indeed, this consideration precludes the IP protection of any database formed within public blockchain.