Blockchain, Smart Contracts and Intellectual Property. Using distributed ledger technology to protect, license and enforce intellectual property rights

Ronny Hauck

Professor, Alexander Humboldt University. Address: 6 Unter den Linden, Berlin 10117, Germany. E-mail: ronny.hauck@rewi.hu-berlin.de

Abstract

For several years, almost everyone has been talking about blockchain. The underlying distributed ledger technology has become (in)famous as the technology behind cryptocurrencies such as Bitcoin and Ether. But what about blockchain and intellectual property like patents and copyright? Could this technology be used for the protection and enforcement of such rights? Which role can smart contracts play in this regard? This article focuses on questions concerning the requirements for provingthe protection of technical inventions as well as on the administration and exploitation of intellectual property rights. The latter could play an important role for intellectual property, which has not been registered or is not subject to registration, such as copyright. For trade secrets, a blockchain could be a useful tool for providing appropriate confidentiality measures. Last but not least, smart contracts in particular could be involved in connection with the transfer and, even more importantly, the licensing of intellectual property and mainly of software.

Keywords

blockchain, distributed ledger technology, smart contracts, intellectual property management, trade secrets, software, digital register, licensing, micropayment.

For citation: Hauck R. (2021) Blockchain, smart contracts and intellectual property. Using distributed ledger technology to protect, license and enforce intellectual property rights. *Legal Issues in the Digital Age,* no 1, pp. 17–41.

DOI: 10.17323/2713-2749.2021.1.17.41

1. Blockchain and smart contracts — technical background and challenges

1.1. Introduction

In its basic form, a blockchain[1] is an open ledger of information that can be used to record and track transactions and which is exchanged and verified on a peer-to-peer network [Clark B., 2018]. This paper analyzes use of blockchain technology in relation to intellectual property[2] with a specific focus on smart contracts. It is, however, not intended to examine questions regarding possible protection of the technologies concerned or of individual components or applications of intellectual property rights, for example to software or a database; see [Yanitsky-Ravid S., Kim E., 2019]; [Hoin-Hein N., Barth G., 2021]. Rather, it is a matter of working out what significance this technology already has or could have in the future — for example in dealing with patent-protected inventions or copyrighted works, as well as its significance for products developed on the basis of such intellectual property.

1.2. Blockchain/distributed ledger technology

Blockchain is the best known and most commonly used distributed ledger technology. Distributed ledger technology is a technology that facilitates an expanding, chronologically ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network. The concept of blockchain was first introduced to the public in October 2008 by a person (or group of persons) who published a paper under the pseudonym "Satoshi Nakamoto" entitled "Bitcoin: A Peer-to-Peer Electronic CashSystem" [Ross E., 2017: 359–360].[3] A blockchain can be understood as a decentralized, i.e. distributed database. It has no central server and thus no central authority that checks and verifies the transactions. From a business point of view, a blockchain is an exchange network

[1] For technical background of blockchain see [Pilkington M., 2016]; [Allessie D., 2019].

[2] For the purposes of this article, the term includes trade secrets. In German law, for example, most academics do not consider trade secrets (*Geschäftsgeheimnisse*) as an intellectual property *right (Immaterialgüterrecht)*, but nevertheless as a type of intellectual property (*Geistiges Eigentum*). Unless otherwise noted, this article is limited to questions of European and German law.

[3] Available at: https://bitcoin.org/bitcoin.pdf (accessed: 24 Feb 2021). Since then Blockchain has developed from version 1.0 to version 3.0. Blockchain 1.0 emphasizes virtual currency, but with Blockchain 2.0 the values being transferred are programmable transactions in the form of smart contracts. Blockchain 3.0 represents the expansion of the technological applications beyond finance and markets.

for moving value between peers, who themselves are functional units in the same layer of a network.

Different types of data can be added to a blockchain, from cryptocurrency (most notably Bitcoin and Ether — ETH) and transactional and contractual information to data files, photos, videos and contract documents. While Bitcoin was designed as a cryptocurrency, several blockchains have been created since then for different purposes and every one of them contains distinctive features Gurkaynak G., 2018: 848]. For example, the Etherum blockchain is a "Turing complete blockchain" [Sergey I., 2018] with the ability to run smart contracts (see below 1.3).

The respective data is written into a "block" as soon as it has reached a certain capacity. This process repeats continuously until the next block is filled. Each block refers back to the previous one, so that a chain of blocks — called a "blockchain" — is created. This leads to a distributed and highly redundant[4] "data archive", which makes it impossible to delete the data. The blockchain is immutable;[5] blockchain records are time-stamped and traceable. Therefore, the real innovation of distributed ledger technology is that it ensures the integrity of the ledger by means of crowdsourcing supervision and removes the need for a central authority, e.g. public registries. In other words, transactions are verified and validated by the multiple computers that host the blockchain (the so-called nodes). For this reason, it is seen as "nearly unhackable," because a cyber-attack would have to strike out (nearly) all copies of the ledger simultaneously in order to change any of the information on it [Clark B., 2018]. In summary, the main features of blockchain technology are data integrity, verification and public transparency of transactions [Allessie D., 2019].

The term "hashing" is also particularly important, as hashes are the central security element in a blockchain. A hash (output) is the result of a transformation of the original information (input). A hash function is a mathematical algorithm that takes an input and transforms it into an output. A cryptographic hash function is characterized by its extreme difficulty to revert, i.e. the recreation ofthe input data solely from its hash value [Pilkington M., 2016].·This sequence of letters and numbers is a kind

[4] Data redundancy: a condition created within a database or piece of data storage technology in which the same piece of data is held in separate places. Available at: https://www.techopedia.com/definition/18707/data-redundancy (accessed: 24 Feb 2021)

[5] However, some scholars dispute whether the term "immutable" accurately reflects nature of the blockchain; a definition of the concept of "immutability" as it relates to the blockchain, aligns with the term "unchangeable" [Walch A., 2017: 736–739].

of unique digital fingerprint, which is always unique for each different data set [Kuchta R., 2017]. As a result, hashing is used for the verification/ validation process of the blockchain, which takes place through so-called “mining” (the creation of a new block).

The blockchain is therefore a procedure in which the falsification and deletion of the content concerned is precluded by the cryptographic encoding of chained entries. This opens up the possibility of tracing economically significant transactions — such as the transfer or licensing of IP — in a tamper-proof manner. Furthermore, actions against counterfeiting in particular could play an important role in the present subject.

1.3. Smart contracts

As mentioned above, using the Etherum blockchain as an example, smart contracts are a mechanism for expressing computations on a blockchain. A single, generally accepted definition of the term “smart contracts” does not exist. According to one widespread view, a smart contract is a program that is stored in a tamper-evident and tamper-proof manner and is guaranteed to execute upon the fulfilment of certain predefined criteria [Szabo N., 1997]; [Raskin M., 2017]. In particular, the program code allows digital assets or representations of physical objects to be reallocated in the form of transactions between two or more parties on the basis of other (external) data not yet known at the time the code was programmed. More generally, such software could also be described as controlling, monitoring and/or documenting legally relevant actions (in particular an actual exchange of services) as a function of digitally verifiable events[6].

As a “computerized transaction protocol that executes the terms of a contract” [Tapskott D., Tapskott A., 2016: 72, 83, 101, 127], smart contracts are a conceivable field of application of the blockchain technology. The idea behind these “intelligent contracts” is — to put it simply — that the contracts can ultimately execute themselves and sometimes act autonomously. Thus, smart contracts allow the performance of transactions without the involvement of third parties. The transactions are traceable and irreversible. One possible example is the granting of usage rights (licenses) for actions with copyright implications on the internet and in particular, the resale of such

[6] However, smart contracts are not “smart” in the sense of (strong) AI, as they are unable to understand natural language or to independently verify whether an event has occurred which is relevant for execution of the smart contract. They also cannot be qualified as “contracts” in the legal sense because they are (just) a computer-programmable ´if/ then´relation and are incapable of taking wider contextual factors into account.

rights (see below 4.3). Another field of use of blockchain technology could be the creation of a system for near-real-time payments for public performances of musical works. Thereby, music licensing could be implemented through smart contracts [McJohn S., McJohn I., 2016: 10, 11].

1.4. Challenges

In general, from a technical point of view, the main challenge prohibiting the widespread adoption of distributed ledger technology for the management of IP rights is the difficulty of explaining and understanding the complexities of the technology itself. Therefore, only applications with simple and easy-to-use interfaces are likely to be accepted and used in the (near) future [Gurkaynak G., 2018: 860, 861].

Furthermore, there are also very specific technical challenges could prevent the technology from being widely used. For example, when using a blockchain for transactions and, in particular, as a (micro-)payment system, a significant technical problem currently facing blockchain technology is the speed with which the respective transactions can be processed, as blockchain is significantly slower than traditional transaction platforms such as VISA or PayPal.[7] In addition, since the users of a blockchain system are also the nodes of the system in a blockchain, each user would need to store massive amounts of data. Despite these concerns, given the rapid technical developments in storage technology in recent years, one can nevertheless hope that software developers will resolve this issue in the near future.[8]

Blockchain technology faces several legal challenges, too. Firstly, it is often difficult to determine which jurisdictions' laws and regulations apply to a given blockchain application, as the nodes of a decentralized ledger can span multiple locations around the world, resulting in an overwhelming number of laws and regulations which could apply to transactions in a blockchain based system [Salmon J., Myers G., 2019]; [O'Shields R., 2017: 190]. Regarding smart contracts in particular, if there is ambiguity as to the location where the contract was concluded, the courts will have to find a method of defining and determining the place of conclusion of the smart contract [Fulmer N., 2019: 185–186]. In addition, the fa.ct that smart contracts do not necessarily require legal enforcement may make them attractive for illegal transactions. Therefore, legal challenges could provide a considerable obstacle to development and widespread adoption of services based on distributed ledger technology.

[7] Ibid, p. 850.

[8] Ibid., p. 861.

2. Protection of technical inventions and trade secrets

2.1. Technical inventions

Technical inventions are (primarily[9]) protected by patents. Article 52(1) of the European Patent Convention (EPC) states that

European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.

Consequently, both novelty and the "inventive step" (better defined as "non-obviousness") [Sai Deepak J., 2010: 410–427]; [Lauber-Ronsberg A., Hetmank S., 2019] are prerequisites for patentability.[10] Article 56 EPC states that an invention shall be considered as involving an inventive step if, having regard to the state of the art, it is not obvious to a person skilled in the art. The invention shall be considered to be new if it does not form part of the state of the art (Article 53(1) EPC).

Decisive importance is therefore attached to the "state of the art". This includes "everything made available to the public by means of a written or oral description, by use, or in any other way, before the date of filing of the European patent application" (Article 54(2) EPC). As this broad wording suggests, the greatest challenge in examining the patentability of an invention is to determine the state of the art and thus to identify all information in the meaning of Article 54(2) EPC. It is not only the status quo in the country of filing that is significant, but also all the publicly available information (the relevant specialist knowledge) worldwide in the field relevant to the technology being applied for a patent. There is no territorial restriction with regard to the publicly available state of the art.

This also applies in US patent law, where — similar to European law — novelty and prior art are also prerequisites of granting patent protection. A patent will not be granted for a technical invention if information about the patented product or process (or the underlying technical solution) was publicly available and thus known before the relevant priority date of the patent, since 35 U.S.C. 102(a) states as follows:

[9] Under German law, technical inventions are also protectable as utility models (*Gebrauchsmuster*).

[10] The requirement to be "susceptible of industrial application" is of least importance since an "invention shall be considered as susceptible of industrial application if it can be made or used in any kind of industry, including agriculture" (see Article 57 EPC), a requirement which is usually easy to fulfil.

A person shall be entitled to a patent unless—(1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention […].

There is also no territorial restriction in US law with regard to information harmful to novelty. The only decisive factor is the accessibility of the relevant information to the public.[11]

As each block of a blockchain contains not only a cryptographic hash of the previous block, but also a timestamp, one conceivable field of application for blockchain technology could therefore be the documentation of the innovation process — the inventive steps that ultimately led to the technical invention worthy of protection. The evidential function of a blockchain could be used in technical developments (which are to be patented as inventions), for example, to document the development cycle of a product and thus the state of the art, or the further development of the product achieved by the invention in question, without gaps — and in a tamper-proof manner.

2.2. Actions against patents

The function of a blockchain as described above (e.g. the documentation of the invention process) could also be used *vice versa* against patents which have already been granted. There are several ways of limiting the scope of the patent or even invalidating a patent (revocation). Under the EPC (see Article 100), an objection can be filed "on the grounds that the subject-matter of the patent is not patentable under Articles 52 to 57", which includes the requirements of "novelty" and an "inventive step"(non-obviousness, see above 2.1). For example, it could be argued against the patent of a third party (and in particular that of a competitor) that a technical solution already belongs to the state of the art, i.e. is not new and does not constitute an inventive step. Based on such information, precisely because of the strong evidentiary function of the information stored in the blockchain, the patent in question could be declared invalid (in whole or in part). It could also be easier for the defendant to prove in a patent infringement process the invalidity of a patent, meaning that it could not be infringed at all. Because, if the defendant files an action for nullity against the patent, the court that decides on the patent infringement (*Landgericht*)

[11] See e.g. In re Wyer, 655 F.2d 221, 226, 210 USPQ 790, 794 (CCPA 1981) (regarding an Australian patent application).

might be more inclined to use this information to initiate the infringement process in accordance with Section 148 of the Code of Civil Procedure in order to wait for the outcome of the nullity proceedings before the Federal Patent Court (the so-called injunction gap).

So far, German courts have been generally reluctant to stay proceedings solely because of parallel pending proceedings on oppositions or nullity. They will only do so if the defendant provides sufficient evidence and arguments to convince the court that there is a substantial likelihood of the patent being invalidated. In a patent infringement lawsuit, the blockchain — or the information stored there — can thus have the function of a both a shield and a sword.

2.3. Co-inventors and R&D-cooperations

As many technical solutions are developed in a team,[12] a tamper-proof blockchain can also be used to prove the exact involvement of individuals in an invention process. This becomes even more complicated if such a team does not consist solely of employees of one company, but also of external persons, for example within the framework of a research and development (R&D) cooperation or even an open innovation process. In practice, the question of who actually participated in the development and to what extent is not always easy to answer. On the one hand, it is often not fully documented who was involved in the invention process at all. On the other hand, it is also not particularly easy to determine, especially when the cooperation has ended, how large the contribution of the participants to the invention actually was.

In R&D cooperations and irrespective of the situation of the co-inventors just described, the aforementioned documentary function of the blockchain can also become important, since it could be established beyond doubt which cooperation partner has made which developments and when. This can considerably facilitate the later assignment of the respective intellectual property developed during the cooperation, the so-called "foreground-IP". In addition, license agreements can be managed within the framework of smart contracts (for licensing of IP through smart contracts see below 4.2), for example with regard to the background-IP of the

[12] In German law, if several people are involved in an invention, they form an inventor community (*Erfindergemeinschaft*). The co-inventors share the right to the invention in accordance with Sec. 6 second sentence of the Patent Act. The relevant law, however, can only be found in the German Civil Code, Sec. 741–758.

parties involved or the later exploitation of the cooperation results [Hohn-Hein N., Barth G., 2018: 1094].

2.4. Protection of trade secrets

It is safe to say that during the process of searching for a technical solution to a technical problem, which, if successful, leads to a patentable invention, extensive technical knowledge (know-how) is created, which does not necessarily flow fully into the invention. In cooperations, such know-how becomes part of the foreground-IP. For companies, however, such knowledge can be just as important and in some cases even more valuable than the patent-protected invention itself. When dealing with trade secrets, it has long been discussed whether trade secrets can be seen as a type of (intellectual) property. This discussion cannot be continued here. It is, however, generally recognized that the essential elements of trade secret protection are confidentiality and (limited) access. Therefore, the person who actually controls the access to the information concerned can be considered its "owner" or "holder".

Given the specifics of the distributed ledger technology (see above 1.2), the blockchain could serve to prove the source of this knowledge and who is actually entitled to this know-how. Additionally, the blockchain could play a role in the protection of trade secrets. Information (know-how) not protected by a patent may nonetheless fall under general concept of a "trade secret" pursuant to Directive 2016/943 (the Trade Secrets Directive) and is only of value to the holder[13] if it is not generally known. In accordance with the requirements of Article 2(1) (a) of Directive 2016/943, only information that

> "is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question"

is protected as a trade secret. This requirement is based on Article 39(2) (a) TRIPS:

> "[such information] is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; not generally known or readily ascertainable".

[13] According to Article 2(2) of Directive 2016/943 "'trade secret holder' means any natural or legal person lawfully controlling a trade secret".

The "holder" must therefore ensure that the information in question[14] does not become public knowledge. This applies accordingly to non-technical information (in particular commercial knowledge such as information about customers, prices, etc.) that can easily have (at least) a similarly high value for a company.

In addition, the holder of such trade secrets can only take civil action against infringers if they can prove that the respective information "has been subject to reasonable steps under the circumstances" to keep the information secret (Article 2(1) (c) Directive 2016/943). The term "reasonable steps" still needs judicial interpretation. This is comparable to US law, where "reasonable efforts" or "reasonable measures" must be proven (cf. Section 1(4) (ii) Uniform Trade Secrets Act and 18 USC Section 1839 (3) (A) Defend Trade Secrets Act respectively).

How valuable the information in question is for the holder or — from a different perspective — what negative consequences disclosure would actually have depends on the individual case. It can be assumed, however, that the more valuable the information is, the higher the requirements will be for "reasonable steps" to keep it secret. Nevertheless, for the adequacy of the measures to keep the respective information secret, the specific (financial) capabilities of the respective company of ensuring effective protection of secrets must also be taken into account. In principle, large companies have better personal and technical resources than small and medium-sized enterprises (SMEs). As a result, the latter are likely to face challenges under the new law, although it should be noted that the Directive pursues the goal of promoting SMEs (see Recital 2 Directive 2016/943). However, this will hardly be possible if the actual feasibility and thus the reasonableness of the measures are not taken into account for SMEs, as otherwise the Directive would ultimately have a negative effect on the protection of trade secrets in the European Union's internal market.

The limited access to the relevant information (the respective trade secret) is made possible by the hash mentioned above (see above 1.2) as the actual security mechanism. Therefore, as a rule, no access restrictions to the blockchain system are necessary ("permissionless" or "public" blockchain[15]). However, the problem with the protection of secrets *by* the block-

[14] According to Article 2(1)(b) of Directive 2016/943, the information has to have "commercial value because it is secret".

[15] As members of the blockchain network are free to negotiate the level of decentralization that the network will have, partially decentralized blockchains are also possible (semi-permissioned blockchain).

chain lies in the fact that the technology is based on a decentralized and ultimately transparent architecture, which may not be compatible with the idea of the protection of trade secrets at all. Protection of trade secrets could therefore only be considered as appropriate if the relevant information is not itself stored, but only the hash. The owner of the unchanged file could then reproduce this hash using an encryption program and prove the sole ownership of the information.

Due to the comprehensive protection against falsification and deletion of information, as well as the possibility to regulate access to it, the blockchain could therefore play an important role in the protection of trade secrets. In addition, the blockchain's function in this respect — to provide evidence that the information has been "subject to reasonable steps [...] to keep it secret" — also provides proof of who actually controls the non-public information and is therefore the "holder" (pursuant to Article 2(2) Directive 2016/943).

Furthermore, it is conceivable not to use a public system (a permissionless blockchain), but instead to employ a system with restricted access, a "private" — or "permissioned" — blockchain, even if this contradicts the original idea of transparent data and information storage. The idea of the blockchain as distributed ledger technology was originally to create transparency by distributing the data records across a network (on a large number of computers), thus protecting the data from falsification, destruction and suppression [Blocher W., 2017: 338]. While the traditional concept of blockchain is an open and anonymous network, there are also "private" blockchains, which pre-screen who is allowed to administer the ledger. Permissioned blockchains act, in contrast to public blockchains, as closed ecosystems, where users are not freely able to join the network, to see the recorded history, or to carry out their own transactions [Dob D., 2018]. Such blockchains are run by specific members of consortiums or companies on a private network (intranet or VPN) [Finck M., 2019: 14,15] and members need to opt-in to the creation of such a network. Additionally, only approved people or computer entities are able to run nodes on the network, validate transaction blocks, issue transactions, execute smart contracts, or read the transaction history.

With regard to trade secrets, a "proof of participation" mechanism must be used to prove special entitlement to participate in the system. It will usually be prudent for the holder of the trade secret to grant the corresponding authorisation solely to trustworthy persons as a central point of legitimation. This limitation of access is therefore the first stage of the "reasonable steps" to keep the information secret, which must be proven in accordance with the provisions of the Directive as desribed above. The evidential value of information stored in such an architecture will, of course, be lower than that of a blockchain with a "genuine" distributed ledger approach.

3. Copyright

In contrast to patent law — patent protection requires that the patent has been granted and published in the patent register — and according to Article 2(2) Berne Convention ("The enjoyment and the exercise of these rights shall not be subject to any formality"), copyright protection for works of art does not arise through a constitutive official act, but solely through the fact that the work in question is created.

In German law, even declaratory registration is not necessary, nor is it possible, as such a register does not exist. In contrary, until the USA joined the Berne Convention in 1989, all works had to be registered in the USPTO's Copyright Register in order to be protected by copyright, meaning the registration was therefore constitutive. Since then, protection in the USA also arises with the creation of a work, but in order to conduct an infringement suit, it is still necessary to register a work created in the USA by a US citizen in the Copyright Register (see Section 411(a) of the Copyright Act).

As a general rule, the copyright holder is the person who created the work (the author). The author must provide proof of actual authorship of a particular work. As already described above in relation to technical inventions, the blockchain could have a documentary function if the process of the creation of a copyrighted work is recorded there [Hohn-Hein N., Barth G., 1092]. Not only would this allow documentation of the ownership of the rights, but also the comprehensible recording of the actual scope of protection for the work, described in detail. The blockchain would thus become a digital register, whereby the entries would have a purely declaratory character.[16] However, such registrations are likely to be far more significant than described above in relation to copyrighted works at their exploitation stage. Registrations of this nature could be even more significant

[16] Platforms like binded.com ("the world's first copyright platform") are based on distributed ledger technology. Authors can upload their copyrighted works (most notably photographs); Binded creates a digital fingerprint of it and writes a permanent record into the bitcoin blockchain. It also provides a "copyright certificate" to prove the ownership of the respective person.

and important for the purposes of documenting the granting and scope of rights to exploit copyrighted works (see below 4).

As already mentioned in relation to technical inventions, the situation in which several people collaborate to create a copyrighted work can be a source of conflict. For example, think of a computer program created by several software developers. In this respect, too, copyright protection is available to all developers collectively. The resulting problems can then be similar to those of the inventor community (see above 2.3). In this case, the storage of information about the creative process in a blockchain could also have the function of documenting the actual contribution of the individual co-authors to the work (the computer program) with high accuracy.

4. Transfer and licensing of intellectual property

4.1. Blockchain as a digital register

A blockchain peer-to-peer network could be used to enable the tamper-proof and erasure-proof recording of transaction histories, such as during the transfer and licensing of intellectual property rights. The intervention of a third (neutral) authority — a private or state intermediary — would then become obsolete [Gurkaynak G., 2018: 855]; [Schrey J., Talhofer T., 2017: 1431]. The blockchain could thus have the function of a digital and trustworthy register, especially in the case of intellectual property rights and/or licenses of such rights for which such a register does not exist, namely in copyright law and more generally for the documentation of sales and licensing transactions.

4.2. Technical IP — transfer, licensing and insolvency procedures

The patent owner or the exclusive licensee can assert claims arising from the patent in their own name, especially in the case of a (presumed) infringement. Therefore, the plaintiff must prove that they are actually the holder of the relevant patent (or at least that they hold an exclusive license). This can be difficult in cases when the patent was aquired from the original owner, because patents are not necessarily sold individually. Instead, entire patent families or even patent portfolios which can consist of a very large number of patents (and patent applications) are often transferred. Furthermore, the assignment of patents is free of any form requirement; in particular, no change to the patent register is required to make the acquisition effective.[17] The relevant change in the register to be requested from the patent office is nevertheless important because the patent register has a presumptive effect with regard to patent ownership.[18] In European law, Rule 22 *et seq*. of the "Implementing Regulations to the Convention on the Grant of European Patents" state that the transfer of a European patent application can be recorded in the European Patent Register. These applies *mutatis mutandis* to the grant or transfer of a license, the establishment or transfer of a right *in rem* in respect of a European patent application and any legal means of execution affecting such an application.

Especially in the case of cross-border patent transfers, commonly there is a failure to document the transfer history and to update the patent register. This can cause significant problems as, before German courts, the plaintiff has to prove in an infringement proceeding that they actually are the holder of the patent which is the subject of the suit, especially if the defendant denies this ownership. Otherwise, the claim will most likely be dismissed as inadmissible owing to a lack of standing (*Prozessführungsbefugnis*).[19] For these purposes, the use of blockchain technology conveniently provides the ability to document such transfers.[20]

Regardless of any impending or ongoing infringement dispute, companies may need to prove that they actually own certain patents. This applies, for example, to start-ups because it can be important for investors to have complete evidence of the actual ownership of patents and patent applications which are crucial to the companys business and therefore essential for the valuation of the company. This function — the proof of ownership by blockchain — applies in a comparable way to corporate transactions, for example in the context of due diligence to determine which intellectual property rights and licenses the company in question actually has.

The question of ownership of patents and patent licenses can also play an important role in the insolvency of a company. Accordingly, in indi-

[17] As an exception, an assignment of a European patent application "shall be made in writing and shall require the signature of the parties to the contract" (Article 72 EPC).

[18] In German patent law, the Federal Supreme Court uses registration as an important indicator of ownership, see Judgement of the Court, 7 May 2013 — X ZR 69/11, 197 BGHZ 196 — Fräsverfahren.

[19] Another view is that the lawsuit would be unfounded because of a lack of ownership (*Aktivlegitimation*).

[20] DLT-based platforms already exist on which intellectual property rights can be traded. The platform LEXIT (www.lexit.com) describes itself as "the first M&A marketplace where anyone can buy and sell IP, code, tech, and companies, via an all-in-one platform powered by blockchain".

vidual cases it may be crucial whether a company actually holds a patent or at least an exclusive license. This is because a simple license would not be protected if the licensor were to become insolvent. As permitted by German law, the insolvency administrator could be inclined to terminate the license agreement and thus eliminate the legal basis of the license, according to the Insolvency Statute, Sec. 103:

(1) If a mutual contract was not or not completely performed by the debtor and its other party at the date when the insolvency proceedings were opened, the insolvency administrator may perform such contract replacing the debtor and claim the other party's consideration.

(2) If the administrator refuses to perform such contract, the other party shall be entitled to its claims for non-performance only as an insolvency creditor. If the other party requires the administrator to opt for performance or non-performance, the administrator shall state his intention to claim performance without negligent delay. If the administrator does not give his statement, he may no longer insist on performance.

The (former) licensee could then no longer invoke a right of use, which could have a significant negative impact on their activities. If, on the other hand, they are the owner of the patent — resulting from a transfer and not a mere licensing of the patent, which can be easily demonstrated through the blockchain — or they are at least the owner of an exclusive license, their legal status would be secure [Pahlow L., 2017: 140]; [Zurth P., 2020: 25].

4.3. Software licenses in the era of "UsedSoft"

As already was noted by Alexander and Peter Hoppen [Hoppen A., Hoppen P., 2018], one highly relevant application of the blockchain is the management of software licenses based on the ECJ´s decision "UsedSoft/Oracle" from 2012[21] and subsequent decisions of national courts.[22] In that particular case, the plaintiff (Oracle) had developed client-server software, which was sold primarily to commercial customers, mostly together with package licenses for at least 25 users. The license agreement granted the purchaser *inter alia* an unlimited (non-exclusive) non-assignable right to use the respective software. The software itself was not sold on a disk or

[21] Judgment of the Court (Grand Chamber), 3 July 2012, Case C-128/11, ECLI: EU:C:2012:407, UsedSoft GmbH v Oracle International Corp.

[22] See e.g. Federal Supreme Court, 17 July 2013 — I ZR 129/08, GRUR 2014, 264 — UsedSoft II; Federal Supreme Court, 19 March 2015 — I ZR 4/14, GRUR 2015, 772 — Green-IT.

another carrier, but was located on a central server. The (non-exclusive[23] and non-transferable) user right to such a program, which is granted by a license agreement for an unlimited period, includes the right to store a copy of the program permanently on a server and to allow a certain number of users to access it by downloading it to the main memory of their work-station computers. An additional maintenance agreement permitted the download of updated versions of the software (updates) and programs for correcting faults (patches) from Oracle's website.

The defendant — the company with the telling name "UsedSoft" — sold "used software licenses" by acquiring "unneeded" licenses to certain software (including the license keys) from the initial purchaser and reselling them. According to UsedSoft, their customers ("second-hand buyers") lawfully acquired the right to download the software directly from the website of the respective manufacturer.

Oracle, as the proprietor of the exclusive user rights under copyright law to those programs, considered the actions of UsedSoft and its customers as an infringement of Oracle's exclusive right of permanent or temporary reproduction of computer programs within the meaning of Article 4(1)(a) of Directive 2009/24 (the so-called Software-Directive). The defendant (UsedSoft) argued that the right to distribute the software had been exhausted, based on Article 4(2) Directive 2009/24:

> The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof.

Therefore, Oracle's customers were entitled to transfer the right of reproduction to the respective programs to third parties — an argument which the ECJ ultimately followed. The Court thus extended the scope of the principle of exhaustion (the so-called 'first-sale doctrine') to encompass software and software licenses, going far beyond the traditional understanding of this principle [Hilty R., 2018: 865].[24] However, in order to

[23] In addition, Oracle's license agreements state that the right to use the programs is "non-transferable".

[24] There has been a long debate about whether the ECJ's broad interpretation of the exhaustion principle/the first-sale doctrine in UsedSoft/Oracle also applies to other digital goods, like eBooks. On the basis of a recent decision of the ECJ, this should be answered in the negative, see Judgment of the Court (Grand Chamber), 19 December 2019, Case C-263/18, ECLI:EU:C:2019:1111, Nederlands Uitgeversverbond and Groep Algemene Uitgevers v Tom Kabinet Internet BV and Others.

solve the problem of the — theoretically conceivable — endless number of copying processes and program copies[25], the ECJ required the first purchaser to make "their" program copy unusable after resale.[26]

It is precisely in this regard — assuming the admissibility of this business model based on the ECJ's assessment — that the blockchain could have an important (evidentiary) function. This could be documented, in particular, by rendering the so-called first copy unusable on the part of the reseller (first buyer). This would put an end to the multiple use [Chohan U., 2017] of the software as required by the ECJ and, in wake of this decision, also by the German Federal Court, which places extremely high demands on such evidence.[27] As blockchain records are immutable and cryptographically secure, there would not be any reason for courts or other authorities to disallow or reject a blockchain record as proof [Gurkaynak G., 2018: 854]. The assignment of a license to an authorized person can be verified by presenting a certificate together with the transaction history, which is verifiable in the blockchain. The respective person, who may have to prove their authorization, has the necessary key for this.

Regardless of the "UsedSoft" situation, the blockchain could play an important role in other aspects of copyright contract law. Similarly to the aforementioned situation for patent licenses (see above 4.2), the proof that a license has actually been granted as well as the scope of that license (and thus compliance with the license conditions, see below 4.4) could be evidenced. In addition, any sublicensing with the creation of a so-called 'license chain' and the further transfer of copyright licenses could be documented by the blockchain as a digital register that is tamper-proof, so that anyone who has to prove their original or derived usage right at a certain point in time would be able to do so [Blocher W., 2017: 339, 340]; [Hohn-Hein N., Barth G., 2018: 1093].

4.4. Scope of IP licenses

With smart contracts, the contractually agreed services and further conditions are recorded using one piece of software. It is not actually a contract, but rather an illustration of one [Kaulartz M., Heckman J., 2016: 618,

[25] Of course, contrary to what the ECJ obviously assumes, a program copy cannot be transferred (and therefore resold). Rather, new copies are made and the reseller sells and transfers the issued licenses via "Used Soft".

[26] Judgment of the Court (Grand Chamber) 3 July 2012, Case C-128/11, ECLI:EU:C:2012:407, UsedSoft GmbH v Oracle International Corp, mn. 78.

[27] See Federal Supreme Court, 17 July 2013 — I ZR 129/08, GRUR 2014, 264 — UsedSoft II: Even a notarial certificate is not sufficient.

621]. The software in question can automatically use blockchain technology to check whether a contracting party has actually performed the owed service. The main function of the underlying technology in smart contracts is to document the obligations to be performed in a verifiable manner and ultimately to monitor their fulfillment. In the very paper where Nicholas Szabo coined the term "smart contracts", he suggested that one application of smart contracts would be to automatically disable a car if the loan payments were not made in timely fashion [Szabo N., 2019].

A license agreement on intellectual property rights can also be designed as a smart contract. In this respect, the underlying software could monitor whether e.g. the licensed patented technology or copyrighted software is only actually used to the extent contractually agreed. Therefore, the licensor could easily prove to the licensee any breaches of contract, which, pursuant to German law, are also violations of the intellectual property right itself.[28] It is also conceivable that the contract will be performed in such a case, for example in the sense that the licensee will no longer granted access to the software in the cloud by the licensor or that at least a corresponding warning is automatically issued. The payment of the license fees could also be processed via blockchain (see below 4.5).

4.5. Equitable remuneration for authors

Another area of application for blockchain technology is micropayment through digital currencies. The right to an equitable remuneration (*angemessene Vergütung*) for the use of the author´s work is one of the main tenets of German copyright law. Copyright Act, Sec. 11 states:

> Copyright protects the author in his intellectual and personal relationships to the work and in respect of the use of the work. It shall also serve to ensure equitable remuneration for the use of the work. (emphasis added)

This principle also forms the basis for Copyright Act, Sec. 32:

(1)The author shall have a right to the contractually agreed remuneration for the granting of rights of use and permission to use the work. If the amount of the remuneration has not been determined, equitable remuneration shall be deemed to have been agreed. If the agreed remuneration is not equitable, the author may require the other party to consent to a modification of the agreement so that the author is granted equitable remuneration.

[28] See Patent Act, Sec. 15(2)(1) and Trade Mark Act, Sec. 30(2). Although there is no such rule layed down in the German Copyright Act, the principle is also applicable to copyright licenses.

(2)Remuneration shall be equitable if determined in accordance with a joint remuneration agreement (section 36). Any other remuneration shall be equitable if at the time the agreement is concluded, it corresponds to what in business relations is customary and fair, given the nature and extent of the possibility of use granted, in particular the duration, frequency, extent and time of use, and considering all circumstances. [...].

It is conceivable that remuneration for copyright-related usage could be processed via internet. This means that license agreements would not only be concluded automatically on a mass basis, but that the remuneration would also be processed at the same time — which is exactly what bitcoins were invented for [Nakamoto S., 2008].[29] The advantage is that the payment is actually case-dependent and usage-related and takes place directly between the user and the rights holder. This is a counter-model to the European and notably German system of copyright limitations[30] with lump-sum remuneration stipulated in framework agreements, which in turn can only be claimed by the collecting societies concerned.[31] Only in a further step, through the distribution, does the rights holder receive their remuneration. In a developed system of smart contracts, the standardization of the statutory limitations to the author´s rights could therefore be dispensed with, at least for private use. Any act of use would, first of all, have copyright implications and a license agreement in the form of a smart contract would be required (unless the right holder were to grant a gratuitous license). In return, the user would pay for the use, which would also be automated. This would make the entire collecting societies system — at least in this respect — obsolete.

Alternatively, collection societies can work with other companies to provide better service to their rights holders in an increasingly competitive

[29] The problem now, however, is that Bitcoin payment fees have risen sharply recently. Available at: https://bitcoinmagazine.com/articles/bitcoin-now-useless-micropayments-solutions-are-coming1/ (accessed: 24 Feb 2021). Therefore, Bitcoins can hardly be considered an inexpensive alternative, particularly to credit card payments.

[30] See Article 5 (Exeptions and limitations) of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. In German law, the limitations of the author´s rights can be found in Chapter 6 (Limitations on copyright through lawfully permitted uses; section 44a et. seq.) of the Act on Copyright and Related Rights.

[31] In German law, collecting societies like GEMA and VG Wort are private, incorporated associations of authors, musicians, publishing houses etc. with the aim of common enforcement of copyrights. Their function is the administration of the rightholder's fee from secondary usage rights (right of reproduction, right of distribution etc.). The general legal priciples are enshrined in the Law on Collective Rights Mangement (Verwertungsgesellschaftengesetz); see also Reinbothe (2015).

market for collecting societies in the EU.[32] An example for using distributed ledger technology in this way is the music blockchain startup Revelator, working with the music recognition service BMAT and the Finnish music collecting society Teosto. The application "Artist Wallet" enables the payment of performance royalties to composers for radio airplay. BMAT runs a music recognition service that uses fingerprinting technology to identify songs being played on various platforms. Revelator maintains a blockchain platform based on Ethereum. The smart contract architecture is designed to enable accurate real-time splits of rights holders' royalty positions, providing enhanced visibility for clearance and settlement of royalty transactions. Payments are automatically distributed to all the stakeholders at the same time.[33] Revelator sends queries to BMAT every two hours. When BMAT returns "play data" for one of the compositions involved in the prototype, Revelator deposits a transaction on its Original Works platform through a smart contract that determines which rights holders get paid and how much. Payments are made in Original Works tokens. The rights holders will be able to convert those tokens to the paper currency of their choice once the project reaches that stage. This system enables near-real-time payments for public performances of musical works instead of the conventional scheme of payments, for example 45 days after the end of each quarter.[34]

5. Enforcement of IP rights and fight against counterfeits

A case decided in June 2018 in the Peoples Republic of China clearly shows that blockchain technology can play an important role in dealing with infringements of intellectual property rights. There, the Hangzhou Internet Court had to decide whether information from a rights holder

[32] Now that European collecting societies are allowed to compete across borders, smaller societies like Teosto need to be innovative to compete with their larger counterparts such as SACEM in France and GEMA in Germany.

[33] Available at: https://www.prnewswire.com/il/news-releases/revelator-launches-the-first-digital-wallet-app-for-artists-and-music-makers-moves-entertainment-industry-toward-instant-royalty-payments-300855100.html (accessed: 24 Feb 2021)

[34] The streaming platform Choon, which provides "service[s] for independent musicians and [a] digital payments ecosystem powered by the Ethereum blockchain". Available at: https://datatransmission.co/news/blockchain-streaming-platform-choon-announces-next-phase/ (accessed: 24 Feb 2021), launched in mid-2017. However, as of late 2019 and due to a "significant downturn in the crypto market", Choon announced a partnership with Emanate, another platform which enables realtime payments and digital contract automation for the music industry based on distributed ledger technology. Available at: https://emanate.live/home (accessed: 24 Feb 2021]

stored in a blockchain about actual violations could be credible evidence.[35] The Court ultimately affirmed this to be the case.

The case was about unauthorized public access to copyrighted content. The rights holder (and plaintiff) had made screenshots of the websites with the disputed publications and had them saved by an external service provider, the evidence preservation platform Baoquan.com. Baoquan uses the Bitcoin blockchain for storage and the blockchain-based document security platform Factom. Baoquan captures images from a target webpage by automatically employing Puppeteer (an open source program by Google) and at the same time acquires the source code of the target webpage by employing curl. To save space, only the hash of the relevant data is saved.[36] This hash can, however, be only reproduced by the person who owns the unchanged original file with the aid of an encryption program.

In the decision, the court dealt extensively with the evidential value of the information stored in this way, e.g. the webpage screenshots captured through Puppeteer that demonstrated the alleged infringing article published by the defendant in 2017 was substantially consistent with the article at issue. It recognized the value as particularly high because the evidence preservation platform was an independent third party. The blockchains used were also considered to be particularly secure due to the number of network nodes involved. The Court stated in particular: "This evidence securing system is equally open to all people and anyone can use the system. Moreover, the operation process thereof is automatically completed by a machine, according to a program preset by the evidence obtaining system. The likelihood that relevant links are tampered with by humans throughout the evidence obtaining and evidence securing process is relatively low. Therefore, the source of the electronic data has relatively high credibility; [...]. In the absence of evidence to the contrary, therefore, this court confirms that the approach by Baoquan.com to parse a domain name for a target webpage to generate and store digital messages by using public open source capture programs from Google is reliable."[37]

This example shows the important role distributed ledger technology already plays in proving infringements of intellectual property rights — and the role it can still play in the future. This is because it is often difficult

[35] Judgement of June 27, 2018-055078. No. 81. Available at: https://go.dennemeyer.com/hubfs/blog/pdf/Blockchain%2020180726/20180726_BlogPost_Chinese%20Court%20is%20first%20to%20accept%20Blockchain_Judgment_EN_Translation.pdf. (accessed: 24 Feb 2021)

[36] Ibid.

[37] Ibid.

to actually prove that an intellectual property right has been violated or — at least — to what extent an infringement has occurred.

6. Summary and outlook

This article points out the importance and potential areas of application of distributed ledger (blockchain) technology in general and smart contracts in particular with regard to intellectual property rights — today and possibly in the future. There is no denying that the new technology poses technical and legal challenges. However, such concerns do not fundamentally speak against the future use of distributed ledger technology in the area of intellectual property.

First, it was shown that the described possibility of seamless and tamper-proof storage of information about the process of invention in the blockchain could be used to document the "state of the art". This is necessary for technical inventions in order to prove the patentability of an invention. Using such information, it would also be possible, however, for patents to be challenged if the protected technology was not new and/or did not go beyond the known state of the art. The related proof of priority could also play a similarly key role with other intellectual property rights, such as design rights and trademarks.

Given the special challenges of co-inventions and in the context of R&D cooperations, through information stored on a blockchain it could also be proven who (and to what extent) contributed to an innovation process, which is helpful for the specific assignment of the result. In the case of works protected by copyright, the creative process could be documented in a comparable way, here in particular to prove the authorship. Overall, the blockchain would thus function as a reliable digital register.

Technical and non-technical information not protected by exclusive rights are of enormous economic importance for companies. However, such information is only really valuable if it is not obvious. The storage of trade secrets in a blockchain could suffice to fulfill the requirement of an effective and, importantly, an appropriate protection of secrets. By using this technology, the strict requirements of the new European law on the protection of trade secrets could be met. The extent to which a blockchain is ultimately able to ensure effective protection of trade secrets (know-how) depends both on the respective technical design and, crucially, on who actually has access to the information concerned.

Another important area of application for blockchain technology and smart contracts lies in the documentation of the transfer of protective rights, the granting of licenses and the transfer of licenses. Such evidence is particularly important for the holder of a legal position, who has to prove the existence of this legal position — and thus an intact "chain of rights" or licenses — for example in order to be able to counter the accusation of unauthorized multiple use. The licensor may have the ability to check whether an intellectual property right (in particular licensed software) has only been used to the extent permitted by the respective contractual framework (licensing agreement).[38] Given the specific situation of the transfer of "used" software, the assignment of a license to an authorized person could become more readily verifiable.

Last but not least: in the case of infringement of intellectual property rights, a recent decision in China has shown vividly the high evidentiary value that can be attributed to the information stored in a blockchain. It remains to be seen to what extent this will also be the case before German and European courts. However, as the Hangzhou Internet Court stated in the case described above: "Technical means like blockchain should be analyzed and determined case by case with an attitude of being open and neutral. Distributed ledger technologies should not be dismissed nor the burden of proof raised because they are novel and complex."

References

Allessie D. et al. (2019) Blockchain for digital government: An assessment of pioneering implementations in public services. In: Pignatelli F. (ed.) JRC Science for Policy Report. European Union. Available at: https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf. (accessed: 24 Feb 2021)

Blocher W., Hoppen A., Hoppen P. (2017) Softwarelizenzen auf der Blockchain. *Computer und Recht*, no 36, pp.337–348.

Chohan U. (2017) The Double Spending Problem and Cryptocurrencies. Available at: https://ssrn.com/abstract=3090174 (accessed: 24 Feb 2021)

Clark B. (2018) Blockchain and IP Law: A Match made in Crypto Heaven? Available at: https://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html. (accessed: 24 Feb 2021)

Dob D. (2018) Permissioned vs Permissionless Blockchains: Understanding the Differences. Available at: https://blockonomi.com/permissioned-vs-permissionless-blockchains/ (accessed: 24 Feb 2021)

[38] In relation to copyright, blockchain technology and blockchain-based smart contracts could also play a future role as a tool in Digital Rights Management; see for a general overiew [Finck V., Moscon V., 2019: 79].

Finck M. (2019) *Blockchain Regulation and Governance in Europe.* Cambridge (Mass.): University Press, 255 p.

Finck M., Moscon V. (2019) Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. *IIC*, no 1, pp. 77–108.

Fulmer N. (2019) Exploring the Legal Issues of Blockchain Applications. *Akron Law Review*, vol. 52, pp. 161–192.

Gürkaynak G. et al. (2018) Intellectual property law and practice in the blockchain realm. *Computer Law Security Review*, vol. 34, pp. 847–862.

Hauck R. (2017) Der Erschöpfungsgrundsatz im Patent- und Urheberrecht, EuZW, vol. 28, pp. 645–649.

Hilty R. (2018) Kontrolle der digitalen Werknutzung zwischen Vertrag und Erschöpfung´. *GRUR*, vol.120, pp. 865–880.

Hohn-Hein N., Barth G. (2018) Immaterialgüterrechte in der Welt von Blockchain und Smart Contract. *GRUR*, vol. 120, pp. 1089–1096.

Hoppen A., Hoppen P. (2018) License on Blockchain: Transferring and Managing Software Licenses on the Ethereum Blockchain, Version 1. Available at: https://github.com/license-on-blockchain/whitepaper/releases (accessed: 24 Feb 2021)

Kaulartz M., Heckmann J. (2016) Smart Contracts — Anwendungen der Blockchain-Technologie. *Computer und Recht*, no 35, pp. 618–624.

Kraßer R., Ann C. (2016) *Lehrbuch Patentrecht*. 7th ed. Munich: Beck,

Kuchta R. (2017) The hash — a computer file's digital fingerprint. Available at: https://newtech.law/en/the-hash-a-computer-files-digital-fingerprint/(accessed: 24 Feb 2021)

Lauber-Rönsberg A., Hetmank S. (2019) The Concept of Authorship and Inventorship under Pressure: Does Artificial Intelligence Shift Paradigms? *GRUR International* no 4, pp. 641–647.

McJohn S., McJohn I. (2016) The Commercial Law of Bitcoin and Blockchain Transactions. Legal Studies Research Paper no 16–13. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874463(accessed: 24 Feb 2021)

Nakamoto S. (2008) Bitcoin: A Peer-to-Peer Electronic CashSystem. Available at: https://bitcoin.org/bitcoin.pdf (accessed: 24 Feb 2021)

O'Shields R*. (2017) Smart Contracts: Legal Agreements for the Blockchain. N.C. Banking Institute,* no 21, pp. 177–194.

Pahlow L. (2017) Patentlizenz und Patentlizenzvertrag. In: Henn/Pahlow (eds.) Patentvertragsrecht. 6th ed. Heidelberg: C.F. Müller, 401 p.

Pilkington M. (2016) Blockchain Technology: Principles and Applications. In: Olleros F., Zhegu M. (eds.) Research Handbook on Digital Transformations. Cheltenam: Elgar, pp. 225–253.

Raskin M. (2017) The Law of Smart Contracts. *Georgetown Law Technology Review,* no 2, pp. 305–341.

Reinbothe J. (2015) Collective Rights Management in Germany. In: Gervais D. (ed.) Collective Management of Copyright and Related Rights. 3rd ed. The Hague: Kluwer Law International, pp. 215–250.

Rosenblatt B. (2019) Blockchain Applications for Music Enter the Bowling Alley. Available at: https://copyrightandtechnology.com/2019/06/15/blockchain-applications-for-music-enter-the-bowling-alley/ (accessed: 24 Feb 2021)

Ross E. (2017) Nobody Puts Blockchain In A Corner: The Disruptive Role of Blockchain Technology. *Catholic University Journal of Law and Technology,* vol. 25, pp. 353–386.

Sai Deepak J. (2010) The Elusive Quest for the Definition of Obviousness — Patent Law's Holy Grail. *IIC*, no 4, pp. 410–427.

Salmon J., Myers G. (2017) Blockchain and Associated Legal Issues for Emerging Markets, EM Compass. Available at: https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F (accessed: 24 Feb 2021)

Schrey J., Thalhofer T. (2017) Rechtliche Aspekte der Blockchain. *NJW,* vol. 70, pp. 1431–1436.

Sergey I. (2018) Scilla: a Smart Contract Intermediate-Level Language. Available at: https://arxiv.org/pdf/1801.00687.pdf (accessed: 24 Feb 2021)

Szabo N. (1997) The Idea of smart contracts. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (accessed: 24 Feb 2021)

Tapscott D., Tapscott A. (2016) *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.* N.Y.: Random House,

Walch A. (2017) The Path of the Blockchain Lexicon (and the Law). *Review of Bank and Fin Law,* vol. 36, pp. 713–765.

Yanisky-Ravid S., Kim E. (2019) Patenting Blockchain: Mitigating the Patent Infringement War. Available at: C:/Users/Juristische%20Fakultät/Downloads/SSRN-id3357350.pdf. (accessed: 24 Feb 2021)

Zurth P. (2020) Lizenzverträge und Lizenzen in der Insolvenz und Einzelzwangsvollstreckung. In: Obergfell E., Hauck R. (eds.) Lizenzvertragsrecht. 2nd ed. Berlin: De Guyter, pp. 183–225.