Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0

Michèle Finck · Valentina Moscon

Published online: 20 December 2018
© The Author(s) 2018

Abstract This article examines the potential and limitations of blockchain technology and blockchain-based smart contracts in relation to copyright. Copyright has long been enforced through technological means, specifically Digital Rights Management. With the emergence of blockchains, many are now predicting a new era regarding the administration and enforcement of copyright through computer code. The article introduces the technology and related potential and limitations while stressing its capacity to act as a form of normative ordering that can express public or private objectives.

Keywords Digital rights management · Copyright · Blockchain · Smart contracts · Private ordering · Permitted uses

1 Introduction

Law and technology have a complex relationship. Technology shapes legal development, while it is also shaped by law. The unfolding of copyright law confirms these dynamics as its development and enforcement have always been closely inspired by the technological state of the art.1 With the emergence and

---

1 Alexander and Gomez-Arostegui (2016). In general, see Goldstein (2003).

M. Finck (✉)
Dr.; Senior Research Fellow, Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: michele.finck@ip.mpg.de

V. Moscon
Ph.D; Senior Research Fellow, Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: valentina.moscon@ip.mpg.de
sophistication of blockchain technology as well as blockchain-based smart contracts, some now perceive a new wave of technological transmutation on the horizon that could have a lasting influence on copyright law. Indeed, it is suggested that these technologies could provide new mechanisms for the management of intellectual property rights that could even take the place of current paradigms.

Copyright law has long leveraged the power of computer code to create binding norms for those that engage with related enforcement systems. Over the past decades, this objective has been achieved through reliance on Technological Protection Measures (TPMs) and Rights Management Information (RMI), two technologies that are key components of Digital Rights Management systems (DRM).²

DRM and generally the technological enforcement of law, spurred by digitalization, datafication, and the online availability of copyrighted materials as well as ubiquitous computing, is transforming our understanding of law. Joel Reidenberg and Lawrence Lessig affirmed two decades ago that computer code is one of many forms of “law” (in the sense of normative constraints) that shape human behavior.³ DRM can in certain scenarios be used as a behavior-constraining force given that computer code can enforce existing legal and contractual rules \textit{ex ante} and in a more efficient manner.

At the same time, technology can also be relied on to circumvent existing legal protections.⁴ DRM has been denoted as an additional layer of paracopyright constraints or technological self-protection – effectively creating a normative regime that can diverge from that designed by lawmakers. DRM as a matter of fact essentially may annihilate legally recognized protections such as exceptions and limitations in the EU and fair use under US copyright law.⁶

As these problematic aspects of DRM attract wide consensus, blockchains and blockchain-based smart contracts are ever more frequently portrayed as the saving grace capable of using technology to enforce copyright law in a better and more balanced manner. Yet this depends on how these technologies are and will be designed. In this paper we provide an early examination of this area. Before introducing blockchain and blockchain-based smart contracts we chart the impact of digital rights management on copyright law taking into consideration the regulation provided for by international copyright treaties. These treaties opened up a tension between public and private ordering in the copyright law domain that has been replicated in national legislations. Examples will be taken from the US and European legal regimes, as they are influential illustrations of regional and national level implementations of international copyright law. Thereafter we provide an

² WIPO Copyright Treaty (adopted in Geneva on 20 December 1996), Arts. 11–12 and WIPO Performances and Phonograms Treaty (adopted in Geneva on 20 December 1996), Arts. 18–19.
³ Lessig (1998); Reidenberg (1998), pp. 553.
⁴ The legal protection of TPMs represents the most controversial area of copyright protection. See Hilty (2005), pp. 103–138.
⁵ Quoting a letter of 16 September 1997 endorsed by 62 copyright law professors characterizing the Digital Millennium Copyright Act (DMCA) anti-circumvention provisions as “paracopyright”, see H.R. REP. No. 105–551 (1998), p. 24.
⁶ Among others see Caso (2006); Fitzner (2011); Dilşen Bulut (2015); and Samuelson (2016).
overview of the expected uses of blockchains and blockchain-based smart contracts as an alternative to current forms of DRM. The article will follow two main paths. Firstly, we will build on the experience gained so far with DRM systems to explore the delicate interplay between public and private ordering in blockchain environments. Whereas this is an important tension in copyright law, it also assumes a broader significance. In particular, we consider regulation of TPMs – *de lege lata* – and highlight – *de lege ferenda* – the need for legal rules to be technology neutral. We explore this point providing some general reflections on the implications of using code as a means of legal enforcement. Secondly, while looking at the prospects of application of blockchain technologies in the copyright domain we evaluate them particularly in relation to supporting an efficient and transparent administration of copyright and neighboring rights.

## 2 Digital Rights Management

In the last decades of the 20th century the information society triggered the dematerialization of copyrighted materials through digitalization while in the early 21st century datafication has reached a tipping point. This has not been without influence on copyright law. The emergence of those phenomena has caused the “fluidity” of digital subject matter leading to a paradigm shift that generated challenges for a copyright legal framework previously based on tangible assets. Digital assets can, in principle, more easily be copied, mixed and shared. At the same time the dematerialization of copyrighted materials has made them more broadly accessible. This has led to a retreat of law in favor of private ordering and self-enforcement as the private sector has used the normative force of code to make it express its own interests and goals, sometimes to the detriment of public policy objectives. DRM systems are a paradigmatic example of this tendency.

### 2.1 DRM Architecture

DRM refers to software and hardware that defines, protects and manages rules for accessing and using digital content (text, sounds, videos, etc.). The first model of DRM was put forward in the late 1990s in the form of a system for controlling the distribution and use of digital material that expressed rules in machine-readable form. These systems have been particularly appealing to the media industry to enforce copyright and neighboring rights protection. DRM systems have evolved over time and can be used in various domains for different purposes. In recent years, for example, the appeal of DRM for producers has been amplified in digital

---

7. We return to the notion of fluidity below.
8. Caso (2016), pp. 145–194.
9. Rosenblatt and Dykstra (2003) and Favale et al. (2016).
10. Stefik (1997), p. 138.
11. Rosenblatt and Dykstra (2003), p. 10.
12. Hughes (2016).
markets by the fact that the datafication and connectivity has extended DRM even to interconnected analogue products. As the Internet of Things progresses and copyright protectable software and databases become embedded in a wider range of goods the effect of DRM systems in economic and social processes may be pervasive.14

DRM has been designed with the aim of giving right holders the broadest possible control over digital content in self-enforcing related terms and conditions of access and use.15 For instance, DRM has been intended to support publishing and selling electronic books, digital movies, digital music, interactive games, computer software and other objects distributed in digital form.16 Policies and business models of right holders are expressed in license agreements that leverage the exclusive rights recognized by copyright and neighboring rights to determine the rules of use of digital material. Contractual terms and conditions are translated into DRM architecture that concretely define how content can be used by third parties and restrict use possibilities accordingly.17 Although there is no standard model of a DRM architecture, DRM solutions typically include a reference policy or business model and technical components for managing content to be protected; creating and managing licenses that specify the rules for consumption of content; tracking usage of content to ensure this is in line with license rules; and submitting packaged content for management by the DRM architecture. These components are also supported by a number of security services. The expectations on these services include guaranteeing the integrity of licenses, protecting content against tampering, authenticating consumers before protected content can be accessed, and safeguarding sensitive data at rest and in transit. These services are implemented to defend against attacks to DRM protocols, against DRM client software, and the software and hardware used to store and render the protected content.18

Relevant components of DRM systems are technological protection measures (TPMs) and rights management information (RMI), which are both the subject of international copyright treaties.19 TPMs include hardware and software to protect the rules and identify the content, the user’s IT system and the user him/herself. The different types of TPM all seek to provide an effective protection mechanism through which content owners may manage the use of their subject matter and access to it by third parties. TPMs can be as simple as a password system, which provides the entry of specific symbols to access a particular subject matter, or more sophisticated, capable of monitoring all conceivable uses of a work.20 The most

13 DRM in combination with the legal protection of technological protection measures applied to software and databases – as will be discussed below – may de facto allow technological protection of data irrespective of the way they are collected.
14 Erickson et al. (2017), p. 2 et seq.
15 See Bechtold (2003a, b), pp. 597–654 and Caso (2006).
16 Rosenblatt et al. (2002), p. 79.
17 Moscon (2013).
18 Favale et al. (2016), p. 294 et seq.
19 WIPO Copyright Treaty (WCT), Arts. 11–12, and WIPO Performances and Phonograms Treaty, Arts. 18–19.
20 See further, Rosenblatt et al. (2002); Armstrong (2006); Meléndez-Juarbe (2009); and Diehl (2012).
widely used TPMs are encryption, digital watermarking, copy control, fingerprinting, access control, authentication key management and other restrictions, all of which enforce conditions upon the users of digital subject matter. RMI is information that identifies content protected by copyright or neighboring rights, the rights owners in such content and the terms and conditions of use associated with it. It may provide the basis for user services, such as information accompanying a radio broadcast that gives right holders track and purchase details about particular songs. The WIPO Treaties protect all such RMI: information about works, phonograms and performances, as well as the identification of authors, phonogram producers, performers or other right holders. Protection also extends to information about terms and conditions of use of content. This may be either details of a license already granted or information about how and under what conditions a license can be obtained.21

In addition, most DRM systems include certain technologies that enable the machine-readable expression of right holders’ policies, in particular rights expression languages (RELs). RELs are technical languages that have specific syntax and semantic vocabulary rules for expressing what kind of uses are permitted, forbidden or obligatory.22 These computer markup languages express a number of permissions such as to stream, copy, delete, modify, embed, execute, export, extract, annotate, aggregate, install, backup, loan, sell, give, lease, play, print, and display in relation to a file. RELs are normally used to express rules contained in the license agreements.23

DRM systems are variegated and their architectures are made up of many hardware and software components which are mostly proprietary and often not interoperable.24 Interoperability of hardware and software is necessary, for example, for users to enjoy digital content from different devices.25 For example, Netflix allows clients using a computer to watch the movies according to the licensing terms governing access and use of content and the interplay between DRM technologies that operate in their computers, the digital movie file, and on Netflix’s servers.26 Also, Netflix’s subscribers can watch the movies with the Netflix mobile application. However, as Netflix fully relies on the Widevine DRM provided by Google,27 it recently announced that devices that are not Google certified or have been altered will no longer work with the latest Netflix App.28 As a result clients

21 Perry (2005).
22 Casanovas (2015) (arguing that RELs emerged from real market needs, reflecting market constrictions, conflicts and potentialities at the same time. Large companies have tried to develop in business their own way of modeling rights. However, the development of REL by means of Ontology Design Patterns or Open Licenses situates the discussion on RELs at the regulatory level) Moscon (2011).
23 See further, Coyle (2004); Hess (2015); and Hohmann (2016).
24 See Koenen (2004), pp. 883–897; Caso (2006), p. 33 et seq.; and Favale et al. (2016), p. 295.
25 Melendez-Juarbe (2009).
26 Ibid.
27 Widevine DRM is a digital rights management component of the Google Chrome web browser and Android MediaDRM. See https://en.wikipedia.org/wiki/Widevine#cite_note-1. Accessed 8 November 2018.
28 https://www.wired.co.uk/article/netflix-app-android-blocked-drm. Accessed 8 November 2018.
visiting Netflix with a device which is not fully interoperable with Netflix-streamed content cannot enjoy movies from that device. This scenario is just one example of how DRM incompatibility can hinder the enjoyment of digital subject matter.\textsuperscript{29}

The lack of interoperability is a consequence of either one company’s decision not to license its technology or, more generally, of the lack of standardization. Indeed interoperability and compatibility among different DRM systems depends on licence agreements between IT companies and standardization processes of DRM components.\textsuperscript{30} However, establishing shared standards in the DRM domain has proven to be difficult.\textsuperscript{31} The various existing proprietary DRM systems are often non-interoperable for at least two reasons. Firstly, companies have preferred to follow market strategies that have been aimed at not sharing some technologies with competitors. This can be seen as the consequence of incentives which strive to establish the dominating, rather an interoperable, standard and benefit from the fruits of such a monopoly (or at least market fragmentation) related to network externalities and lock-in effects.\textsuperscript{32} Secondly, the diversity of digital content to be protected (e.g. video games, music, movies and texts) and the related variance in the relevant level of protection has made it difficult to develop a unitary standardized system.\textsuperscript{33}

However, some have argued that although lack of interoperability limits users’ experience, DRM interoperability is not always desirable.\textsuperscript{34} To the extent that interoperability increases the network of devices and content within the reach of copyright owners, a world with interoperable DRM systems may consequently expand content control and further increase copyright owners’ control at the expense of otherwise legitimate and flexible uses. As will be explained in the following, DRMs can limit the range of uses a person can make with the digital content as a result of de facto elevation of copyright owners’ control over content.\textsuperscript{35} In this sense, increasing interoperability between digital goods and devices should be balanced with measures allowing users’ rights to access and use digital content and flexibility. At the same time, it has been noted that, if the content industry had incentives to allow that balance among control and flexibility, then it might have

\textsuperscript{29}See further, Melendez-Juarbe (2009).
\textsuperscript{30}Rosemblatt and Dykstra (2003) and Melendez-Juarbe (2009).
\textsuperscript{31}It is worth noting here, however, that the World Wide Web Consortium (W3C), the industry body that oversees development of HTML and related Web standards, has recently published Encrypted Media Extensions (EME) as an official Web standard. EME provides a standard interface for DRM protection of media delivered through the browser. EME defines how Web content can work with third-party Content Decryption Modules (CDMs) that handle the proprietary decryption and rights-management portion. See https://arstechnica.com/gadgets/2017/09/drm-for-html5-published-as-a-w3c-recommendation-after-58-4-approval/. Accessed 7 November 2018. The new standard may allow DRM systems to hook directly into users’ browsers. That way, Netflix and other streaming services could protect their content without making users install plugins like Flash or Silverlight. But in other ways, EME’s approval raises concerns. It has been argued that by approving this standard, W3C is giving major browser developers and content providers too much power over what users can do. See Docotorow (2017).
\textsuperscript{32}Caso (2006) and Melendez-Juarbe (2009).
\textsuperscript{33}Hughes (2016); Favale et al. (2016).
\textsuperscript{34}Melendez-Juarbe (2009).
\textsuperscript{35}Ibid.
incentives to develop an interoperable DRM standard, as interoperability is an important dimension of flexible use.\(^\text{36}\)

### 2.2 DRM Between Public and Private Ordering

DRM is an early example of how computer code can be leveraged as a means of public as well as private ordering. On the one hand, these measures give expression to elements of the copyright law regime, meaning that they are a code-based enforcement mechanism of legislative provisions providing right holders with exclusive rights. Copyright law seeks to create a balance between authors’ and users’ interests. Authors should be rewarded for their work as a means of incentivizing creativity, whereas knowledge should also be openly available.\(^\text{37}\) As a consequence, despite recent legislative trends aimed at extending the scope and duration of copyright protection,\(^\text{38}\) most national copyright systems recognize that copyright protection ought to be balanced with human rights, such as the right to privacy, freedom of expression, freedom of research and education, access to information and the right to participate in the cultural life of community.\(^\text{39}\) The most important limits to copyright protection reflecting that balance include: that protection is guaranteed only if works are original; protection covers only the expressive form and not the content; the first sale doctrine and the exhaustion principle; that exclusive property rights can be subject to compulsory licenses; that exclusive rights are extinguished after a certain number of years when the subject matter of protection falls into the public domain; and copyright permitted uses such as exceptions and limitations.\(^\text{40}\)

On the other hand, DRM is a form of private ordering as the private sector has largely used these mechanisms to implement its own objectives, sometimes resulting in the disregard of legal protections such as limitations and exemptions or even in the creation of a factual exclusivity over digital subject matter not eligible for copyright protection.\(^\text{41}\) DRM can indeed neutralize limits enshrined in law. Furthermore, in a mass-contract situation (which is the normal situation in the entertainment and culture digital market) licensors can model terms and conditions in their own favor, limiting the rights of the licensee to use the subject matter of protection.\(^\text{42}\) Moreover, contractors in mass-markets cannot negotiate the terms of the license with the licensor individually, which has led to overly restrictive conditions.\(^\text{43}\)

---

\(^{36}\) Ibid.

\(^{37}\) Both the TRIPS Agreement and the Development Agenda of WIPO recognize that copyright and other forms of intellectual property are grounded on public policies that may encompass development objectives. See in particular the Preamble of the TRIPS Agreements.

\(^{38}\) Caso (2006), p. 82.

\(^{39}\) On the interactions between human rights and intellectual property see further, Geiger (2015).

\(^{40}\) For a comparative analysis of limits to copyright law see Guibault (2002), pp. 15 et seq, and Hilty and Nérisson (2012).

\(^{41}\) Hilty (2018), pp. 10.

\(^{42}\) The debate on this matter dates back to the 1990s. Among others see Nimmer (1999), p. 17.

\(^{43}\) Merges (1997), p. 116 and Goldstein (1997), p. 865.
With regard to copyright permitted uses, the example of academic publishing is emblematic.\textsuperscript{44} Some publishers have converted to an e-only business supply, meaning that print versions are no longer available. Academic authors often grant publishers exclusive rights; therefore, publishers are the single source of academic subject matter and can limit use activities contractually and technically, including uses that are permissible based on statutory limitations or fair use.\textsuperscript{45}

Also, right holders offering e-books can restrict the number of times a book can be copied or printed. Alternatively, they can prohibit all copying even if the original purchaser agrees to delete their own copy.\textsuperscript{46} Under such conditions it is impossible to transfer the e-book to third parties without transferring the reading device itself. In this business model, the exhaustion doctrine (or first-sale doctrine), which allows a book, movie or music that is legally purchased to be passed on to any third party without infringing copyright law, is challenged.\textsuperscript{47}

These examples illustrate that private ordering by code enhances the potential for abuse or misuse of an artificially created factual exclusivity. At the same time these examples also highlight that law sometimes struggles to keep up with digitalization. Going back to the example of the exhaustion doctrine (or first-sale doctrine),\textsuperscript{48} these rules mainly reflect the widely accepted rationale of addressing the inherent contrast between exclusive rights in works and neighboring rights, and the free circulation of legally acquired goods. Exhaustion and first-sale doctrine rules were developed in a technological and economic environment in which the enjoyment and circulation of copyright-protected works presupposed their incorporation in physical carriers. These doctrines were essentially connected to the circulation of physical goods (such as, for example, books, records, etc.) and the right to enjoy the works embedded in those goods was inherent in the good itself. However, the digitalization of content has changed the modes of circulation and enjoyment of works. Both political opportunity and the legal suitability of “digital exhaustion” is challenged.\textsuperscript{49} In this regard it has been questioned whether exhaustion rules are a better way to grant the effective

\textsuperscript{44} On the academic publishers’ business models, see Moscon (2015).
\textsuperscript{45} A relevant debated example in this field is Text and Data Mining (TDM). TDM refers to comparatively new analysis techniques to automatically assess large amounts of digital information by means of computers, thereby generating new knowledge (in particular by identifying correlations or trends). In this case even if modern copyright laws were to provide for a statutory license for TDM, the provision might be ineffective at promoting an automated search if publishers contractually and technically impede TDM. The current proposal by the European Commission for the modernization of copyright in the single digital market includes an exception for TDMs which, if not mandatory, could be contractually and technically prohibited by right holders. See Art. 3 Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM 2016 593 final. See further, Margoni and Dore (2016) and Geiger et al. (2018).
\textsuperscript{46} Hilty (2018), p. 17.
\textsuperscript{47} Ibid, pp. 17–18.
\textsuperscript{48} These legal institutions follow a similar path although their conceptual structure and functioning are not fully comparable. Exhaustion and first-sale doctrine rules were developed in a technological and economic environment in which the enjoyment and circulation of copyright-protected works presuppose their incorporation in physical carriers. These doctrines were essentially connected to the circulation of physical goods (such as, for example, books, records, etc.) and the right to enjoy the works embedded in those goods was inherent in the good itself.
\textsuperscript{49} See further in Mezei (2018) and Hilty (2016).
operation of this area of law and businesses related thereto, creating a balance between the interests of the right owner and those of society (users). Some have recently argued that economic and legal challenges to these doctrines in the digital context provide a foundation for reconsidering exhaustion rules, suggesting that other areas of law might help in finding the abovementioned balance in the digital environment (e.g. antitrust law, consumer law).50

2.3 Controversial Outsourcing to Private Ordering in Copyright Law

National and international law have legislated with a view to limit users’ ability to circumvent some DRM measures. The treaties on copyright and neighboring rights adopted within the framework of the World Intellectual Property Organization (WIPO) in December 199651 impose obligations to provide adequate legal protection and legal remedies against the circumvention of effective TPMs and the removal or alteration of RMI.52 Attention was devoted to technological measures deployed to protect the interests of right holders.53 These provisions parallel the substantive rules protecting copyright law and copyright neighboring rights in the sense that they safeguard the effective operation of technological means affording the exercise of copyright in the digital environment.54 It is worth noting here that TPMs are individual technologies that protect works and other subject matter, while the term DRM, as explained above, describes more complex protection systems that use technological, contractual and statutory protection concurrently.55 A comprehensive regulation of DRM is not provided. States fulfilling international obligations have adopted national schemes such as the US Digital Millennium Copyright Act56 or the European Union’s Information Society Directive (InfoSoc Directive).57 There legislative acts were enacted to implement the WIPO Treaties. Article 6 of the InfoSoc Directive contains the most general anti-circumvention provision in the European legal framework.58 The InfoSoc Directive also harmonizes some aspects of copyright law across Europe.

---

50 See Perkins (2015).
51 WIPO Copyright Treaty (WCT), Arts. 11–12, and WIPO Performances and Phonograms Treaty, Arts. pp. 18–19.
52 It is important to note that for some technologies it is unclear whether they fall under the definition of TPMs or RMI. Digital watermarks, for example, are used to embed rights management information into digital works. If an attacker removes a watermark such behavior violates RMI protection. However, digital watermarks may also be part of a copy control system: if the watermark is removed the copy control system is rendered ineffective. See Bechtold (2016), p. 474.
53 See Senftleben (2016), pp. 93–139.
54 Ibid p. 130.
55 See Bechtold (2016), pp. 421–490.
56 DMCA (1998), p. 2860.
57 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. See Caso (2006), p. 125 et seq.
58 Some other provisions may be found in Art. 7(1)(c) of the Computer Programs Directive (Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs) and in Art. 4 of the Conditional Access Directive (Directive 98/84/EC of the
US and European legislation exceeds international requirements and has been criticized for several reasons, including failing to clearly highlight the necessary functional link between technical measures protection and copyright protection.\(^{59}\) The danger therefore is the excessive extension of the protection of technical measures even beyond the boundaries of exclusive rights.\(^{60}\) Nonetheless, both schemes introduce strict sanctions for those who violate anti-circumvention rules.\(^ {61}\) Indeed, while the legal protection of technical measures is incisive, the law on the inverse situation where contracts and technical measures are used to override copyright limitations is weak. The current legislative framework does not offer effective means to limit private ordering based on contracts and technical measures, irrespective of the potential of such means to override limits to copyright exclusivity.\(^ {62}\)

If we limit our focus to the legally permitted uses of protected subject matter (e.g. exceptions and limitations in the European legal framework and the fair use doctrine in the US), and leave aside for example the factual protection of non-protected material that should be in the public domain, one important issue is whether and how legislators reconcile legal, copyright-permitted uses with DRM. In fact, the technical prohibition of such uses – e.g. the use of works for scientific or educational purposes – is one of the typical ways in which right holders try to extend exclusivity beyond the scope intended by copyright protection.\(^ {63}\) Firstly, it is uncertain to what extent international copyright treaties allow contracting parties to protect technical measures, even in cases where the act of use which is prevented by such measures is permitted under a copyright limitation. It has been argued that the treaties might be interpreted as allowing the contracting parties to give preference to technical measures except in cases where the affected limitation is mandatory.\(^ {64}\) However, international copyright treaties provide only a few instances of mandatory copyright-permitted use.\(^ {65}\) At the national level, copyright legislation quite often does not provide a clear distinction as to whether a permitted use is mandatory. Derogations from copyright-permitted uses may therefore be governed by contract

---

Footnote 58 continued
European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access).\(^ {59}\) With regard to the DMCA, see Burk (2013), available at: https://ssrn.com/abstract=320961 or http://dx.doi.org/10.2139/ssrn.320961. Accessed 16 October 2018. As for the InfoSoc Directive see Dusollier (2001).\(^ {66}\)

Hugenholtz et al. (2007).\(^ {61}\) For a comparative overview, see ibid.\(^ {62}\) Hilty (2018), p. 31.\(^ {63}\) See Samuleson (1999), pp. 504–566; with regard to the European legal framework see generally, Guibault (2002).\(^ {64}\) Senftleben (2016), pp. 93–139.\(^ {65}\) In the international copyright legislation only few exceptions are mandatory, namely the right of quotation in Art. 10(1) of the Bern Convention. Also Art. 7 of the Marrakesh Treaty obliges contracting parties to take appropriate measures to ensure that the legal protection of technical measures does not prevent blind, visually impaired or print disabled persons from enjoying the limitations set forth in the Treaty.
law, and copyright-permitted uses can be overridden through technical or contractual means (or a combination thereof).

Focusing on the European legal framework, the InfoSoc Directive provides very narrow and to some extent uncertain answers against the abuse of technical protection measures. Article 6 of the InfoSoc Directive implements Arts. 11 WCT and 18 WPPT. As mentioned above, Art. 6(4) regulates the relationships to copyright exceptions or limitations. It is important to note first of all that Art. 6(4) specifically forbids the beneficiaries of copyright exceptions or limitations from circumventing technological measures and distributing the tools needed for such circumventions on their own. The consumer who circumvents the TPMs, even for the purpose of exerting an exception or limitation, would still be responsible for violating the anti-circumvention rules. Compared to other anti-circumvention provisions around the world, the European solution is restrictive. The US, for example, has only considered the solution to exempt the user when the circumvention carried out relates to legitimate fair use.

Article 6(4) lists certain exceptions which Member States should ensure that their beneficiaries can enjoy even if TPMs apply. More precisely, the first principle laid down in the Directive is to entrust the right holders with the task of reconciling TPMs with the safeguarding of exceptions. Adoption of “voluntary measures” by right holders appears to be the preferred solution. In the absence of “voluntary measures” taken by right holders, Member States must take appropriate measures to ensure that users can enjoy the listed exceptions, even if TPMs apply. The intervention of lawmakers is thus subsidiary to that of right holders. However, as already mentioned, the aforementioned obligation is not provided for all exceptions and limitations but only for those listed in Art. 6(4). Also, the Directive does not define the “voluntary measures” to be undertaken by right holders. Some commentators have considered “building copyright exception by design” as one example of “voluntary measures”. The right holders could devise the technological measures as to accommodate some copyright exceptions and limitations. This approach, however, has been criticized with respect to its feasibility considering that copyright-permitted uses require a nuanced understanding of contextual and external circumstances which rigid computer code may be unable to replicate.

Further it is important to note that Art. 6(4) is very limited in scope. In fact, the limitations or exceptions to copyright listed in the InfoSoc directive are optional for Member States. If Member States do not implement exceptions under Art. 6(4), the mechanism provided for in this provision is meaningless.

---

66 For details see the country reports, in Hilty and Nérisson (2012), pp. 197–289.
67 See Dusollier (2001) and Reichman et al. (2007), p. 47 et seq., available at: http://ssrn.com/abstract=1007817.
68 See further Dusollier (2001).
69 Similarly to the Australian provisions see Fitzpatrick (2000), pp. 214–228.
70 Article 6 proved to be the most controversial of the entire Directive. See Guibault (2002), p. 220.
71 See Dusollier (2001).
72 Burk and Cohen (2001), p. 56; see also, Felten (2003), pp. 57–58.
73 Dusollier (2001), p. 74.
applicability of exceptions and limitations depends directly on the methods of distribution to the public chosen by the right holder. Article 6(4) establishes that where works and other subject matter have been made available on demand and access is conditioned on the formation of a contract, right holders are not obliged to undertake any activity to ensure that users can benefit from the exceptions and limitations, even though provided for by law. In other words, and this is the most important restriction, Member States are not allowed to take any legislative action at all if the right holders offer technologically protected content over the Internet and access is conditional on the conclusion of an agreement.

This shift of copyright from public to private ordering enabled by both contracts and technological measures is highly controversial. Many scholars criticized the approach of the European legislator, arguing that it conflicts with the very nature of exceptions and limitations.

The copyright domain accordingly confirms the ability of computer code to function as a means of private ordering. Its use has altered the factual availability of existing legal protections. It has also made possible a compression of external limits to copyright law that can be found in other fields of law such as competition law, including consumer protection. Right holders may in fact use DRM as a lever to influence market dynamics. Code can represent a strategic barrier to entry in addition to a contract and the rules protecting the technology that facilitate its use, to erect strategic barriers even in secondary markets. This has been discussed, for example, when DRM is embedded in a computer platform (think of the well-known case of video game consoles or operating systems), projecting effects both on the platform market and on the complementary goods market. The technological standard may become the lever to raise barriers to market entry.

The use of computer code to enforce copyright legislation has accordingly generated a number of limitations and controversies. In light of such shortcomings,
blockchain-based smart contracts are discussed as a new form of code to be taken into account as a potential alternative to existing systems.

3 Blockchain and Smart Contracts

In recent years, blockchain (also referred to as “Distributed Ledger Technology” or DLT) and blockchain-based smart contracts have been touted as suitable alternatives to current systems of DRM that could replace the latter. Much hope is placed in these instruments in light of the controversies associated with DRM that we have outlined above. In this section we introduce these instruments before outlining associated promises.

3.1 Blockchain Technology

The first blockchain was created to provide the technical infrastructure of Bitcoin in 2009. At the time, the technology itself was considered to be merely a by-product of the cryptocurrency and the term “blockchain” does not even figure in Satoshi Nakamoto’s famous White Paper. Rather than being a completely novel technology, it is better understood as an inventive combination of existing mechanisms. Indeed, nearly all of its technical components originated in academic research from the 1980s and 1990s.

3.1.1 Technical Primer

In essence, a blockchain is a shared and synchronized digital database that is maintained by an algorithm and stored on multiple computers such that each stores a complete copy of the database. Blockchain networks achieve resilience through replication. The ledger’s data is resilient because it is simultaneously stored on many computers, so that even if one or several nodes fail, the data remains unaffected. In light of such replication, there is no single point of failure or attack at the hardware level.

The technology gets its name from the fact that it is usually ordered as a chain of blocks. Each block groups together multiple transactions and is then added to the existing chain of blocks. Data is grouped into blocks that, upon reaching a certain size, are chained to the existing ledger through a hashing process. The ledger’s

85 Whereas there can be technical nuances between a blockchain and DLT, they are used as synonyms here for the sake of simplicity and in accordance with conventional usage.
86 Nakamoto (2018). Nakamoto is the pseudonymous mastermind behind Bitcoin.
87 Narayanan and Clark (2017).
88 It is worth noting that some chains operate with a distinction between full and lightweight nodes whereby only full nodes store an integral copy of the ledger from the first block whereas lightweight nodes only store those parts of the ledger of relevance to them.
89 It is worth noting that as the technology evolves, some projects are adopting alternative forms of data storage.
90 A hash is a one-way cryptographic function, designed to be impossible to revert. The hash creates a unique fingerprint that represents information as a string of characters and numbers.
blocks have different key components, including the hash of all transactions contained in the block (its “fingerprint”), a timestamp, and a hash of the previous block (which creates the sequential chain of blocks).[^1]

Because blocks are continuously added but never removed, a blockchain can be qualified as an append-only data structure. Cryptographic hash-chaining makes the log tamper-evident, which increases transparency and accountability.[^2] Indeed, where the hash linking one block to another changes, the hash of that block, as well as of all subsequent blocks does, too.

The replicated data stored in blocks is synchronized through a consensus protocol that enables the distributed network to agree on the current state of the ledger in the absence of a centralized point of control.[^3] Through this process, data is chronologically ordered in a manner that makes it difficult to alter data without altering subsequent blocks.

It must be noted that despite these general commonalities, blockchains vary widely in their technical and governance configurations. An important distinction is that between “public and permissionless” as well as “private and permissioned” blockchains.[^4] In public and permissionless blockchains, anyone can join the ledger simply by downloading and running the relevant software – no permission is needed.[^5] Moreover, anyone can download the entire ledger and view transaction data. Permissionless blockchains rely on open source software so that anyone can download it and participate in the network without the need for prior approval by a gatekeeper. Conversely, on such ledgers, transactions are publicly auditable, which ensures transparency but minimizes privacy.[^6]

Blockchains can, however, also be private and permissioned, which means that an administrator needs to grant permission to individuals wanting to maintain a node. The key distinction between permissioned and permissionless blockchains is that while one needs access permission to join the former, this is not necessary in respect of the latter. Rather a single party or a consortium acts as a gatekeeper. Permissioned blockchains can be internal to a specific company or joint venture (which is why they are also often referred to as “private” or “enterprise” blockchains). It is accordingly important to bear in mind that there is a wide range of different blockchain technologies that may be more or less suitable for various objectives. Indeed, blockchains are better thought of as a class of technologies.

[^1]: Antonopoulos (2017).
[^2]: Felten (2018).
[^3]: Consensus denotes the mechanisms that coordinate data held by the various nodes, providing assurance to network participants that their versions of the ledger are consistent and accurate.
[^4]: While blockchains can be private and permissionless or public and permissioned, at this stage the most frequent combinations are public and permissionless and private and permissioned, which we accordingly also focus on.
[^5]: This is true at least in theory as over time informal restrictions for participation in mining (of an economic nature) and software governance have emerged.
[^6]: See further Finck (2018), Chapter 4.
3.1.2 The Functional Perspective

For our purposes, the relevant question is not so much what blockchain is but what it can do. It is imperative to realize that blockchain is a general-purpose technology, meaning that it can be used for a wide variety of uses. This is so because it is both a database (essentially an accounting book) and a programmable platform on which other applications can run.

A blockchain is a replicated database that is updated in a decentralized manner. This database can be used independently, such as to record transactions in cryptoassets or register information, for instance in a supply chain setting. Here, the blockchain serves as a common asset registry, an innovation in database design that either directly stores data or links to data. These shared accounting systems can be used by different entities to standardize and link data and “enable credible accounting of digital events”. This in turn enables the coordination of information between many stakeholders.

A distributed ledger can furthermore host a wide range of second-layer applications. The applications deployed on a DLT infrastructure reflect the underlying infrastructure’s characteristics of resilience, decentralization and tamper-evidence. While a blockchain only ever stores data, this data can represent anything we believe and agree it represents. Over time, different forms of digital assets have emerged that are still nothing but raw data. Such assets can purely have on-chain value (as in Bitcoin) or be the avatar of a real-world asset, whether a good (such as a token representing a house), a service (such as a voucher for a service) or an entitlement (such as a legal right). Blockchain is sometimes labeled “the Internet of Value” as it is expected to disrupt the online circulation of value as they allow for value-transfers that dispense of intermediaries. To enable much of these projects, smart contracts are needed.

3.2 Smart Contracts

In essence, a smart contract is self-executing computer code that automatically processes its inputs when triggered. It is essentially a small computer program that is deployed on a blockchain. Thus while smart contracts are currently being avidly discussed in relation to blockchain, similar mechanisms have been used for a long time, also by DRM systems. As explained, DRM technology essentially embedded copyright law into digital files by limiting the user’s ability to view, copy, play, print, or otherwise alter the works. For example, digital audio files encrypted with DRM technology were not subject to the double-spending problem because they contained a basic smart contract, which referenced a centralized network (that is, for example, Apple’s server programmed to enforce the iTunes Store Terms and

---

97 Matzutt et al. (2018).
98 Bitcoin is essentially data that is valuable because people have come to believe it is.
99 In essence, a token can be defined as data that can represent whatever we believe and agree it represents, including licensing terms and remuneration.
100 Cortese (2016).
Conditions). Beyond this rather basic definition there is little consensus as to what this terminology really refers. It is worth noting that depending on the adopted definition, smart contracts are not necessarily linked to blockchain technology. Given that they are discussed in relation to distributed ledgers in the literature we introduce below, we will also examine them as such here.

To some, a smart contract is simply a piece of computer code with specific characteristics. Vitalik Buterin portrays smart contracts as “cryptographic ‘boxes’ that contain value and only unlock it if certain conditions are met”. In the blockchain context, a smart contract is “programmed logic that runs on a ledger-like distributed system in response to transaction submission”. From a technical perspective, smart contracts are thus simply computer programs that can be consistently executed by a network of computers without the need for an intermediary. Because of their distributed nature and thus guaranteed execution, smart contracts are resilient to tampering, which makes them appealing in many scenarios including the transfer of value.

Yet, because these technical tools can be relied upon to automate transactions typically governed by contract law (such as value transfers) smart contacts can be useful tools in a contractual setting. Nick Szabo indeed coined the term “smart contract” in 1994, to denote “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”. Szabo envisaged the creation of computer software resembling contractual clauses to connect parties in a fashion that would make it difficult for one party to unilaterally terminate an agreement. Seen from this perspective, a smart contract can be a Ricardian contract, the objective of which is to create contracts that can be read by humans and machines alike. Indeed to some, a smart contract is “a computer program that both expresses the contents of a contractual agreement and operates the implementation of that content, on the basis of triggers provided by the users or extracted from the environment”.

The main value proposition of smart contracts is that of their automated execution. As second-layer applications, smart contracts benefit from the tamper-proof nature of the underlying blockchain infrastructure that anchors their automated execution. Given that many blockchain nodes run smart contract code, it “is not controlled by – and cannot be halted by – any single party”. Smart contracts execute automatically and cannot be halted unless this option is

---

101 Kiviat (2015), pp. 605–608.
102 See further, Finck (2018), chapter 1.
103 Halaburda (2018).
104 Buterin (2015), p. 13.
105 https://medium.com/@Clause/really-smart-and-legal-contracts-a77fcd1d0d10.
106 Bartoletti and Pompianu (2017), p. 494.
107 Ibid, p. 494.
108 Szabo (1996).
109 Ibid.
110 See Grigg (1996).
111 Idelberger et al. (2016), p. 167.
112 De Filippi and Wright (2018), p. 29.
specifically built into the code. This enables transactions in situations devoid of human or institutional trust, lowers transaction costs and reduces counterparty risk and interpretative uncertainty. Once an agreement has been translated into code, the intervention of a party or intermediary (other than the respective oracle) triggering contractual execution is replaced by the software’s automated execution.

Where smart contracts are used to automate the execution of contractual obligations, performance is thus hard-wired into the code. For example, the software can be used for the automatic transfer of collateral in the event of default. Automated execution of course not only provides benefits but also disadvantages. Where software executes automatically, unwanted transactions can no longer be rolled back. This can be problematic, such as when a party lacks legal capacity or a party decides to default on its obligations. Modifications, such as those mandated by law or court decisions also cannot easily be accommodated. Through these characteristics, smart contracts promise to trigger efficiency gains particularly attractive in commercial settings, including in relation to copyrighted materials.

3.3 Blockchain Technologies in the Copyright Domain

The potential of blockchain as a general-purpose technology is currently being experimented with in many domains, including copyright law. Over the past months and years variegated suggestions as to how the technology could be deployed for the management of copyrighted works and neighboring rights objects have been voiced by industry and in the academic literature. In this section, we provide a cursory overview of expected application of these technologies. We organize the following overview around three main drivers leveraging the main characteristics of blockchain technologies. The first driver revolves around the potential capacity of blockchain technology to precisely identify a digital asset and thereby counter the problem of digital “fluidity”. The second driver is related to the ability of blockchain technologies to foster transparent and disintermediated transactions. The third axis focuses on the potential of blockchains to be developed as a DRM system. Finally, in the second sub-section we introduce some structural limits of blockchain technologies such as the so-called “garbage-in garbage-out” problem.

3.3.1 Prospects for Application

Firstly, it has been argued that DLT could be used to create artificial scarcity in the digital market. Indeed in the copyright domain tokens may represent various

\footnote{It is worth noting that many projects seek to make this possible, such as smart contracts arbitration.}

\footnote{For an overview of the advantages of smart contracts, see Giancaspro (2017), p. 33; Holden and Malani (2017), pp. 21–24.}

\footnote{An oracle is an information provider exogenous to the smart contract, which provides information on whether an execution-relevant event has occurred. Oracles can be based on human or machine intelligence.}

\footnote{Yermack (2017), p. 26.}

\footnote{See further, Finck (2018), chapter 3.}
elements including a copy of a protected work. This may solve a number of issues related to the fluidity of digital objects and create new business models. This may lead to the commodification of digital works and thereby allowing the creation of new markets. Some projects have already been implemented, in particular in the field of artworks leveraging the fact that blockchain technologies make digital artworks more attractive for collectors. It has also been speculated that these developments create the necessary preconditions for flourishing, technologically-enabled secondary markets for digital content.

DLT may also enable the precise tracking of certain digital assets (through tokens) that could be used as evidence of authorship and provenance. In relation to attribution, hashing can create a unique fingerprint of copyrighted material that allows verification of authorship and that the creative work existed at a given time without revealing the actual contents. The hash allows monitoring of provenance in through recording ownership and usage. DLT has been presented as a “revolution in how to keep track of rights”. Tokens can encode information including the terms of use of protected material (such information can be mentioned under the definition of RMI). For unregistered intellectual property (IP) rights such as copyright and neighboring rights, blockchain technologies offer the benefit of providing a time-stamped record of its conception, use and qualification requirements. For example, the hash may facilitate evidence in court cases concerning copyright authorship and violation of the terms of use.

Blockchains’ characteristics provide an opportunity to conceive of a global registry for copyright and neighboring rights. Indeed only the existence of a global registry holding RMI would allow for the development of potential benefits into real benefits of blockchain and smart contracts as described in the following paragraph. In this regard it is worth mentioning the project currently implemented by PRS for Music, ASCAP and SACEM which aims at improving data accuracy for right holders. This point will be further developed in the next section.

---

118 Bodó et al. (2018), pp. 311–336.
119 Clark (2018)
120 Ibid, p. 314.
121 See Zeilinger (2016).
122 Savelyev (2018), pp. 4–12.
123 O’Dair (2016), pp. 11–25.
124 Ito and O’Dair (2018) pp. 3–8.
125 O’Dair (2016), pp. 11–25.
126 Bodó et al. (2018).
127 https://offchainlabs.com/.
128 Bodó et al. (2018), pp. 14–15.
129 See further https://www.prsformusic.com/press/2017/prs-for-music-ascap-and-sacem-initiate-joint-blockchain-project. Several other projects are flourishing in this domain such as that carried out by Soundreef. See further https://cryptonomist.ch/en/2018/11/09/soundreef-bitcoins-blockchain-copyright-protection/. Some have raised criticism concerning those projects arguing that most of them are specific marketing actions which do not empower the real potential of blockchain technologies, fostering instead new forms of intermediation. See the arguments of Matteo Fedeli Director of Music Division at SIAE
Secondly, there is the prospect of transparency and cost savings related to smart contracts as once a user purchases the digital asset from a website, the smart contract can be triggered immediately so that all other actions – e.g. payment of royalties to right holders – are automated. Combined with digital currencies, this enables micropayments, which could change pricing models in relation to copyrighted materials. Micropayments – meaning the payment of a small sum, such as EUR 0002 – is currently not an economically viable solution as transaction fees exceed the price itself. The advantages of this method are manifold: “...”

Footnote 129 continued

(Societa’ Italiana Autori ed Editori) as reported by the press https://www.dday.it/redazione/28573/diritto-dautore-soundreef-blockchain-siae. Accessed 14 November 2018.

130 Tresise et al. (2018), p. 149–151.
131 Ibid.
132 Savelyev (2018), p. 4–12.
133 De Filippi and Wright (2018), p. 76.
134 Tresise et al. (2018), p. 153.
135 Ito and O’Dair (2018) pp. 3–8.
136 Heap (2017).
137 Bodo´ et al. (2018), p. 6, 7.
138 Ibid.
prospect. Sometimes the role of intermediaries goes further than the mere management of legal tools being more related to marketing strategies. In any case, for the “direct-to-fan” model to take hold, solutions need to be devised that can provide a user-friendly form of smart contract management, which does not require the user to personally code the smart contract. It should be noted that some are already working on corresponding solutions.  

Smart contracts may also play a role in standardizing licensing terms and conditions for copyright works across uses and jurisdictions. Standardized smart contracts, the terms of which can be described in comprehensible language, augment transparency and reduce barriers to using contracts for transactions. The technology could also be used to generate custom smart contracts with the terms of license payment and even its split between various beneficiaries. 

Thirdly, some believe that DRM itself may be disrupted by blockchain technology. A number of projects are already underway in this domain. Sony recently applied for a patent for a DRM solution based on blockchain. Kodak launched a similar project, KodakOne, which is aimed specifically at photographers and agencies. Whereas over one trillion photos are uploaded to the web each year, most of them fall into the category of orphan works because it is burdensome for photographers to administer image licensing, infringement detection and reporting. KodakOne seeks to change this by creating an image rights management platform, combined with tokens (to manage instantaneous royalty payments) and smart contracts (to document licenses).

These early initiatives underline that blockchain can serve to create a hard-to-amend record of initial ownership with smart contracts being encoded to license the use of copyrighted works. Here, smart contracts are deployed to automate and standardize copyright-related transactions (such as use and exploitation of content as well as remuneration) in relation to blockchain-based tokenized elements. Smart contracts would be modelled to hold, execute and monitor contractual code. The idea is that smart contracts would be used to establish and self-enforce copyright agreements such as licenses, and provide information about rights in copyrighted materials.

Highlighting that traditional DRM solutions rely on single points of failure, are expensive, can be overcome by a single hacker and interfere negatively with consumer expectations, blockchains’ resilience-through-replication is appealing. It is important to note, however, that automated licensing through smart contracts is not to be confused with traditional DRM systems which always involve control of access and use of digital subject matter. Blockchains may offer right holders greater

---

139 On the development of such models, see further Goldenfein and Leiter (2018).
140 Bodó et al. (2018), p. 5.
141 Savelyev (2018), pp. 4–12.
142 Bogna (2018).
143 https://kodakone.com/ico/kodakcoin-ico.html. Accessed 12 November 2018.
144 Bodo et al. (2018), p. 2.
145 Neuburger (2018).
146 Ibid.
security and stronger protections against possible attackers including copyright infringers that seek to access the digital asset. User rights would be encoded on a blockchain. Connected systems would then verify these rights and decrypt the related copyrighted content where appropriate. A smart contract would then be used to allocate access to the digital asset via tokens (such as bitcoin, ether, etc.) that reside on the chain, the role of which consists in facilitating remuneration and payments.

Blockchains do not hold the copyrighted digital asset itself in light of the technology’s limited processing capabilities but rather facilitate a smart contract that contains information regarding related rights and permissions. However, when users use a work through their device, they trigger communication with the distributed ledger. The DRM system can scan the record for the necessary permission and give the user access to the acquired work. For example, if the user has purchased a limited-duration license, the system can consult a trusted timeserver and compare the time with the contract terms coded on the blockchain and take away access once the user’s license has expired. Blockchain technology could therefore control use-rights and just as is the case with current DRM systems, smart contracts do not necessarily encode legally permitted copyright uses. We will return to this point in the following section.

After having summarized the main themes revolving around copyright management by means of blockchain uses, it is worth stressing some structural limitations of blockchain technologies.

### 3.3.2 Structural Challenges

An initial structural weakness is seen in relation to those projects that would not only use blockchain as a technical infrastructure (such as to have a time-stamp for new work) but also cryptocurrencies to support new payment structures. Here, it must be noted that a severe limitation exists in the form of the value fluctuations that at present characterize these systems. The lack of stability of cryptocurrencies indeed currently makes them unappealing for use in royalty payments. While innovations such as pegged cryptocurrencies could solve this, for the time being this remains a prospect for the future.

A further partially related issue is that of network effect. In order to unleash the full potential of a new blockchain-based copyright management system, it needs

---

147 Ibid.

148 Tresise et al. (2018), pp. 149–151.

149 It must be noted that one of the main questions is where copyrighted works themselves will be stored. Storing digital content off-chain creates an issue of accessibility of such content and challenges the effectiveness of the blockchain solutions. It is, however, impracticable to do so considering the limited scalability of these systems. See Savelyev (2018), p. 13.

150 Ibid, pp. 149–151.

151 Ibid, p. 144.

152 Ibid, pp.149–151.

153 Ito and O’Dair (2018), pp. 3–8.

154 Savelyev (2018), pp. 17–18.
to be used by a large number of right owners and cover a sufficient amount of copyrighted works. As the number of users increases, the system will become even more valuable and able to attract a wider user base.\footnote{Ibid.} However, it is not yet clear what the threshold of a sufficient number of users will be in order to begin to disrupt the existing status quo.\footnote{Ibid.} Therefore in the field of copyright law, adoption is one of the challenges in the implementation of blockchain technologies.

Furthermore, blockchains are unable to solve the double-spending problem off-chain. Where the on-chain token is simply the avatar of an off-chain good, it cannot prevent that copyrighted material such as a physical book is copied or sold without updating the relevant information on the ledger. This is a serious limitation in relation to many of the projects that are currently being suggested. Once copyright is transferred outside the network, records in the ledger no longer provide a reliable certificate of ownership.\footnote{Ibid., pp. 3–8.} Many of the proposed solutions are only feasible where such out-of-system transfers are not possible.

Blockchains and blockchain-based smart contracts could moreover be used as a means of copyright infringement. Indeed, they could facilitate the distribution of infringing content in an encrypted form on a peer-to-peer network on a permanent and append-only ledger.\footnote{See Neuburger (2018).} Actual peer-to-peer file sharing of copies of works is difficult to realize in light of blockchains’ technical limitations so that tokenizing access to the infringing content emerges as a more attractive alternative, transaction costs permitting.

Blockchains are append-only ledgers on which information can only be changed in extraordinary circumstances. They are unable to solve the garbage-in garbage-out problem.\footnote{Savelyev (2018), pp. 14–16.} Authenticity of information that is not native to the blockchain simply cannot be guaranteed at the moment of registration.\footnote{Ito and O’Dair (2018), pp. 3–8.} This raises problems, such as where information relevant to copyrighted works is entered incorrectly (either maliciously or mistakenly). Unless technical and governance processes capable of remedying this fact are provided, this remains a severe limitation of the resulting system. It is accordingly unclear how copyright information that was entered incorrectly (whether intentionally or mistakenly) could be altered.\footnote{Ibid., pp. 3–8.} This is, of course, a general concern in relation to blockchains’ tamper-evident nature replicated the “garbage-in garbage-out problem”. Systems using these mechanisms must therefore carefully ponder how this point can be addressed in their systems and governance design.

\section*{4 Assessment}

Above, we have portrayed the possible benefits and limitations of using blockchain and blockchain-based smart contracts as a means of copyright administration. These...
technologies raise several legal issues in the field of copyright and beyond\textsuperscript{162} pinpointing the complex relation between copyright, technology and public policy. It is now opportune to return to the theme of code as a means of public or private ordering examined previously. Indeed, given that these technological tools are based on computer code, just as with DRM, they have the potential to also be leveraged as a means of private ordering to the detriment of legally-protected public policy goals such as access to knowledge. Computer code is one of the many forms of law (in the sense of normative constraints) that shapes human behavior.\textsuperscript{163} Langdon Winner exposed the “politics” of technology over three decades ago, highlighting that technological design choices become part of the wider framework for public order.\textsuperscript{164} The malleability of computer code as a means of expressing normative objectives and constraints is accordingly well known. The normativity of computer code indeed governs the behavior of those that engage with it. Just as law, computer code is also strongly shaped by the objectives and intentions of its creators. What distinguishes both mechanisms, however, is that computer code, unlike law, is enforced in an \textit{ex ante} fashion, meaning that save for the technologically skilled, those exposed to it have no option other than compliance.

The regulatory force of computer code is a central consideration to be kept in mind when pondering the implications of blockchains and blockchain-based smart contracts for copyright law and beyond. In relation to copyright, computer code has long been used as a means of regulating users’ actions.\textsuperscript{165} We have noted above that in current DRM systems, legally-protected public policy objectives have been partly displaced. Historical experience accordingly teaches us to be alert as to how and by whom blockchain code will be used. Whereas the technology could be used to enable more decentralized and fairer means of administering rights and sharing digital content, it could also be relied on to strengthen private interests including those of (potential) new intermediaries emerging in this space.

Blockchains and smart contracts have an extraordinary regulatory capacity. First, the protocols of distributed ledgers enforce their creators’ normative choices. This can be leveraged by public and private actors alike to create an environment for transactions that adheres to specific rules, which may or may not reflect applicable law. Second, applications running on blockchains, most notably smart contracts, are self-enforcing, automating compliance with a pre-determined rule-set, the execution of which cannot be stopped.\textsuperscript{166} The technology is thus a forceful illustration of Lessig’s “code-is-law” paradigm, highlighting that it could be used to either enforce or undermine law.

Blockchains and blockchain-based smart contracts could be employed by right holders in view of strengthening existing systems or creating new ones. For example, as mentioned above in relation to DRM there have not been incentives to

\textsuperscript{162} Some of those issues are comprehensively tackled in Bodó et al. (2018), pp. 8–10.

\textsuperscript{163} Lessig (1998) and Reidenberg (1998), p. 553.

\textsuperscript{164} Winner (1986), pp. 19–39.

\textsuperscript{165} Caso (2008), p. 70.

\textsuperscript{166} Goldenfein and Leiter (2018) arguing that a new legal field is emerging around blockchain platforms and automated transactions.
create DRM architecture including copyright permitted uses thereby limiting flexibility of use of content. At the same time, in relation to DRM, there have not been private interests to converge towards a single DRM system producing at least some components based on secret technologies.\textsuperscript{167} This was mostly due to the attempt of establishing the dominating, rather than interoperable, standard and benefiting from the advantages brought by such a market fragmentation.\textsuperscript{168} As explained in the previous sections, DRM interoperability may be desirable to the extent digital content and devices are balanced with measures allowing users to access and use digital content according to legal copyright limitations. As interoperability is an important dimension of flexible use, if the content industry had incentives to allow the balance among control and users’ flexibility, then an interoperable DRM standard might be foreseeable.\textsuperscript{169}

These examples clearly showcase that technological infrastructure is developed according to the interests of private companies which, unless specific incentives or legislative constraints are put in place, often disregard users’ interests. These issues also remain a concern in relation to blockchain technology. For example, although there are already ongoing efforts at the level of the International Standards Organization to address standard interoperability this remains an unresolved problem.\textsuperscript{170} Standard setting may be crucial for the establishment of a blockchain infrastructure that allows making the best use of the technology. And the public regulator may have an important role in fostering this purpose.\textsuperscript{171}

As a consequence, it is worth considering the introduction of statutory safeguards to foster copyright balance as current legal frameworks are no longer seen as sufficient to guard against misuse of technological enforcement. This has led to suggestions that lawmakers make permitted uses mandatory and irrevocable against contracts and technological self-protection.\textsuperscript{172} Some have suggested a more radical solution in the form of a user-rights approach – a framework for analyzing limits on permissible uses set by private ordering.\textsuperscript{173} This could restore copyright balance as users’ interests could not be threatened by expansive licenses and technological self-enforcement.

Further, proposals of “fair use by design” are suggested as a counterbalancing measure.\textsuperscript{174} Through this approach, public policy considerations would form part of systems architecture, similarly to how the EU’s data protection framework imposes requirements on data protection by design and by default.\textsuperscript{175} This would enable the

\textsuperscript{167} Melendez-Juarbe (2009).
\textsuperscript{168} Ibid.
\textsuperscript{169} Ibid.
\textsuperscript{170} https://www.iso.org/committee/6266604.html.
\textsuperscript{171} Bodó et al. (2018), p. 6.
\textsuperscript{172} Hilty and Moscon (2018).
\textsuperscript{173} See further Elkin-Koren (2015) and Favale (2012).
\textsuperscript{174} Elkin-Koren (2017), p. 22.
\textsuperscript{175} Article 25 GDPR.
incorporation of values into systems architecture by default.\textsuperscript{176} Yet, there have been concerns regarding the feasibility of such approaches considering that copyright-permitted use requires a nuanced understanding of contextual and external circumstances that rigid computer code may be unable to replicate.\textsuperscript{177} Elkin Koren, however, considers that sophisticated machine learning techniques are now capable of realizing such solutions.\textsuperscript{178} Such algorithmic enforcement may be relied upon in the realm of blockchain technologies. Through their respective set-up, these technologies express the “code-is-law” paradigm in setting very precise rules of engagement. Time will tell whether the relevant regulatory set-up is determined by the private or public sector.

Blockchain technology, furthermore, also has the potential to be used as a public copyright blockchain registry, favoring the development of a secure global repertoire database of works and other subject matter.\textsuperscript{179} As explained in the previous section, this would facilitate transparency, the remuneration of right holders and accessibility of works.\textsuperscript{180} The current lack of a trustable database including RMI causes several problems such as conflicting claims on the same works and generally a lack of a share of royalties for authors, artists, songwriters and publishers. In the music industry the lack of transparency and questionable royalty trails is partly due to faulty or non-existent data or simply a lack of sharing relevant data. Using different proprietary databases, which are not interoperable with each other is one of the obstacles for data sharing.\textsuperscript{181} Control of data and namely RMI over works and other subject matter is often perceived as a source of power.\textsuperscript{182} At the same time getting clean metadata and reconciling against other data sources remains a massive problem for many CMOs around the world. It is no secret that CMOs have incomplete and inaccurate RMI.\textsuperscript{183} Nonetheless there have been numerous concerted efforts to try to overcome this problem, yet all such projects have failed. It has been argued that given the interest in having a natural monopoly on data, such failures are likely due to lack of trust in the group who proposes running these projects.\textsuperscript{184}

\begin{thebibliography}{9}
\bibitem{176} See Nissenbaum (2011), p. 1367 (arguing that artefacts embody political and ethical values and discussing the limits of regulation by design); Nissenbaum (2001), p. 120 (arguing that the moral properties of systems, such as bias, anonymity, privacy and security must be attended to by engineers who are developing computer systems).
\bibitem{177} Burk and Cohen (2001), p. 56; see also Felten (2003), p. 57, 58.
\bibitem{178} Elkin-Koren (2017), p. 1100.
\bibitem{179} There is a project on a global database that has, however, collapsed. See Silver (2016), p. 43.
\bibitem{180} The issue of blockchain as a public registry for copyright law and neighboring rights has been addressed by Tresise et al. 2018, pp. 147–148. When dealing with registration systems, the authors also highlight potential issues related to prohibition of mandatory formalities under Art. 5(2) of the Berne Convention for the Protection of Literary and Artistic Work. On this issue generally see van Gompel (2013).
\bibitem{181} Savelyev (2018), p. 5.
\bibitem{182} Silver (2016), p. 50.
\bibitem{183} Ibid.
\bibitem{184} In 2014 despite concerted efforts over several preceding years, a project to create a Global Repertoire Database (GRD) collapsed. Its creation was initiated by the EU Commissioner Neelie Kroes who created Global Database Repertoire Working Group (GRD WG) in September of 2008. In December 2010, it
\end{thebibliography}
For this reason, blockchain has potential relevance to artists, labels, publishers and major music institutions like CMOs. Some consider that blockchain could take over all the functions of CMOs, making their services almost completely unnecessary. Smart contracts would collect and distribute rights in almost real time according to pre-agreed rules put in place by right holders. The desirability of such a scenario, however, clashes with the various functions of CMOs, which go beyond the mere management of rights. CMOs indeed may assume different functions, such as the development of legal and technological tools to support authors and users, that might not have the technical skills to do so independently. Thus, the benefit of using blockchain in this context is more about reconsidering the existing copyright management systems that run through CMOs. Blockchain can support CMOs which, however, will need to rethink their role.

The above highlights that the technology could enable a more disintermediated and fair era of copyright management. To illustrate, smart contract-based micropayments could trigger more efficient remuneration models for the benefit of both users and right holders, or alternatively to charge a micropayment which then goes to an intermediary every time the page of a book is turned. Indeed, while some fear these tools might be used simply as a means for corporations to strengthen existing systems and power structures, a strong innovation ecosystem has emerged that strives to design smart-contracts-based solutions that would provide practical avenues of transposing the ideals of decentralization and disintermediation associated with blockchain technology to the realm of copyright management and enforcement. These include solutions whereby artists gain more control over their work. While a major concern in this domain is the inability of most individuals to code smart contracts on their own, solutions using user-friendly interfaces are issued a set of recommendations, where the group suggested that the GRD should provide access to authoritative, comprehensive, multi-territory information about the ownership and control of the global repertoire of musical works, and that it should be openly available to songwriters, publishers, Collective Rights Management (CRM) organizations, and other potential users. See "Recommendations For: The Way Forward For the Development of a Global Repertoire Database". GRD-077, Global Repertoire Database Working Group, 2010, p. 4. See generally, Milosic (2015).

ASCAP, SACEM, and PRS For Music Initiate Joint Blockchain Project To Improve Data Accuracy For Rightsholders. See further, https://www.ascap.com/press/2017/04-07-ascap-sacem-prs-blockchain. Accessed 12 November 2018.

Silver (2016), p. 43.

See Gervais (2018), pp. 349–356 (arguing that collective management organizations (CMOs) are, first and foremost, copyright and related rights licensing bodies managing vast sums of money. That does not, however, define the entire scope of their activities. For example, the 2014 EU Directive on collective management notes that CMOs “play, and should continue to play, an important role as promoters of the diversity of cultural expression”). See Directive 2014/26/EU on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market (Barnier Directive). In the US it is worth mentioning the recently approved Music Modernization Act which creates a formalized not-for-profit body to administer the mechanical licensing of compositions streamed via digital service providers (DSPs).

CMOs in the EU are regulated by the Barnier Directive.

See the above-mentioned project currently carried out by PRS for Music, ASCAP and SACEM.

De Filippi (2016).
emerging that would allow creators to issue content licenses or split ownership rights in a manner compliant with applicable law,\textsuperscript{191} without reliance on centralized authorities nor the need to code related arrangements themselves.\textsuperscript{192} If such initiatives prove to be successful they could indeed inaugurate a new era of copyright management that remedies some of the shortcomings associated with current systems.

However, as already mentioned, blockchain technologies could also be relied on to control digital assets as a stronger form of DRM. If copyrighted materials were once available unless proven to be infringing, increasingly these materials are managed by smart contracts, whether in the form of DRM or blockchain-based mechanisms. Algorithmic copyright enforcement has led to the paradigmatic change where unless explicitly authorized by the right holder any use is prohibited. This would foster the emergence of normative scenarios in which all that is not expressly forbidden is permitted.\textsuperscript{193} Largely steered by private interests, algorithmic enforcement has changed methods of online consumption of digital content and provided pervasive control.\textsuperscript{194} Smart contracts in the form of DRM have been widely criticized for promoting a private order that is not offset by adequate mechanisms to protect the public interest in accessing unprotected content or protected subject matter in case of permitted uses.

5 Conclusion

The origin of DRM and blockchains is noticeably distinct. Whereas the former results from industry efforts to advance corporate interests, the latter initially emerged in the peer-to-peer cryptoanarchist Bitcoin community. Nonetheless, the same points of tension that surfaced in relation to DRM and copyright law are also likely to arise in the context of copyright-management solutions grounded on blockchains and blockchain-based smart contracts. This is an important point to keep in mind as these solutions develop further. At this stage, DLT remains an immature, and hence malleable technology.\textsuperscript{195} Current projects remain at a proof-of-concept stage, making it difficult to predict how copyright-related uses thereof will develop. The specific implications further hinge on which solutions are developed, and also on the precise configuration of the chosen DLT infrastructure. Yet, this very immaturity and related malleability also provide an opportunity to design systems wary of repeating the mistakes of the past and more capable of providing an appropriate balance of the interests of various actors. Indeed, there is a

\textsuperscript{191} See the OpenLaw project for artworks. A description is available at https://medium.com/@OpenLawOfficial/modernizing-art-with-blockchains-6cba4694833d. Accessed 9 November 2018.

\textsuperscript{192} https://github.com/mitmedialab/OpenMediaLegalHack/wiki/How-To-Use-OpenLaw, https://ujomusic.com/faq. Accessed 14 November 2018.

\textsuperscript{193} Casanovas (2015), p. 123.

\textsuperscript{194} On the tension between private and public ordering in copyright law see Cohen et al. (1998) and Elkin-Koren (2005).

\textsuperscript{195} See further, Finck (2018).
danger that blockchains, just as DRM, will be used primarily as a means of private
ordering that does not account for public policy objectives. This factor must be kept
in mind amidst a current rethinking of copyright rules and related discussions
concerning mandatory permitted uses. Further, as blockchain standards are being
developed, it is important to safeguard that such standards also promote public
policy objectives. This is an important point of general significance because in the
digital economy, standards increasingly take the role of law. In order to address
these challenges and ensure responsible innovation, we recommend interdisci-
plinary research and multi-stakeholder conversations in order to make sure that
these new technologies do not simply become DRM 2.0 but rather improve the
current state of affairs.

Acknowledgements Open access funding provided by the Max Planck Society.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0
International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, dis-
tribution, and reproduction in any medium, provided you give appropriate credit to the original
author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were
made.

References

Alexander I, Gomez-Arostegui T (2016) Research handbook on the history of copyright law. Edward
Elgar Publishing, Cheltenham
Antonopoulos A (2017) Mastering bitcoin. O’Reilly, Farnham
Armstrong TK (2006) Digital rights management and the process of fair use. Harvard J Law Technol, 20:
49. Fall 2006; U of Cincinnati Public Law Research Paper No. 07-10. https://ssrn.com/abstract=
885371 Accessed 30 Oct 2018
Bartoletti M, Pompianu L (2017) An empirical analysis of smart contracts: platforms, applications, and
design patterns. In: Brenner M et al (eds) Financial cryptography and data security. Springer, Berlin
Bechtold S (2003a) The present and the future of DRM – musing on emerging legal problems. In: Becker
E, Buhse W, Günnewig D, Rump N (eds) Digital rights management. Technological, economic,
legal and political aspects. Springer, Berlin, pp 597–654
Bechtold S (2003b) Digital rights management in the United States and Europe. Am J Comp L
52:323–382
Bechtold S (2016) Information Society Directive. In: Dreier T, Hugenholtz PB (eds) Concise European
copyright law. Kluwer Law International, The Hague, pp 421–490
Bodo B, Gervais D, Quintais PJ (2018) Blockchain and smart contracts: the missing link in copyright
licensing? Int J Law Inf Technol. https://doi.org/10.1093/ijlit/eay014
Bogna J (2018) Sony develops blockchain system for digital rights management. https://cryptoslate.com/
sony-develops-blockchain-system-for-digital-rights-management/. Accessed 18 Oct 2018
Burk DL, Cohen JL (2001) Fair use infrastructure for rights management systems. Harv. JL Tech
15:42–83
Burk DL (2003) Anti-circumvention misuse. UCLA Law Rev 10:1095–1140. https://doi.org/10.2139/ ssrn.320961
Burk DL (2005) Market regulation and innovation: legal and technical standards in digital rights
management. Fordham L Rev 74:537–573
Buterin V (2015) Ethereum white paper. A next generation smart contract & decentralized application
platform. http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_ and_decentralized_application_platform-vitalik-buterin.pdf. Accessed 13 Aug 2018
Casanovas P (2015) Conceptualisation of rights and meta-rule of law for the web of data. Democracia Digital e Governo Eletrônico n. 12: 18–41. https://ssrn.com/abstract=2633365. Accessed 8 Nov 2018

Caso R (2006) Digital rights management. Il commercio delle informazioni digitali tra contratto e diritto d’autore. Digital re-release, Trento. http://eprints.biblio.unitn.it/4375/1/Roberto.Caso_DRM.pdf. Accessed 17 Oct 2018

Caso R (2008) Digital Rights Management: problemi teorici e prospettive applicative: atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007. Quaderni del dipartimento di Scienze Giuridiche. Trento

Caso R (2016) Il diritto d’autore dell’era digitale. In: Giovanni P (ed) Il diritto dell’era digitale. Il Mulino, Bologna

Clark B (2018) Blockchain and IP law: a match made in crypto heaven? http://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html. Accessed 18 Oct 2018

Cohen JL (1998) Lochner in cyberspace: the new economic orthodoxy of “rights management”. Mich L Rev 97:462

Coyle K (2004) Rights expression languages: a report for the Library of Congress. http://www.loc.gov/standards/relempart.pdf. Accessed 10 Oct 2018

Cortese A (2016) Blockchain technology ushers in “the internet of value”. https://newsroom.cisco.com/feature-content?articleId=1741667. Accessed 3 April 2018

De Filippi P (2016) How Blockchain can support complement, or supplement intellectual property. https://github.com/COALAIP/specs/blob/master/presentations/COALA%20IP%20Report%20-%20May%202016.pdf. Accessed 13 Dec 2018

De Filippi P, Wright A (2018) Blockchain and the law. Harvard University Press, Cambridge

Diehl E (2012) Securing digital video: techniques for DRM and content protection. Springer, New York

Dils¸en Bulut G (2015) Adaptation of copyright to the information society. Wissenschaftlicher Verlag Berlin, Berlin

Docotorow C (2017) Amid unprecedented controversy, W3C greenlights DRM for the web. https://www.eff.org/deeplinks/2017/07/amid-unprecedented-controversy-w3c-greenlights-drm-web. Accessed 7 Nov 2018

Duke science, technology & innovation paper No. 24. p 47 et seq. http://ssrn.com/abstract=1007817. Accessed 18 Oct 2018

Dusollier S (2001) Exceptions and technological measures in the European Copyright Directive of 2001. IIC 34(1):62–75

Elkin-Koren N (2005) What contracts cannot do: the limits of private ordering in facilitating a creative commons. Fordham L Rev 74:375–422

Elkin-Koren N (2015) Copyright in a digital ecosystem: a user-rights approach. In: Okediji R (ed) Copyright in an age of limitations and exceptions. Cambridge University Press, Cambridge. https://ssrn.com/abstract=2637027. Accessed 18 Oct 2018

Elkin-Koren N (2017) Fair use by design. UCLA Law Rev 64: 22. https://ssrn.com/abstract=3217839 Accessed 12 Nov 2018

Erickson K, Rodriguez Perez J, Sinha S (2017) How much do consumers value interoperability? Evidence from the price of DVD players. https://ssrn.com/abstract=2998767 or http://dx.doi.org/10.2139/ssrn.2998767. Accessed 2 Nov 2018

Favale M (2012) The right of access in digital copyright: right of the owner or right of the user? J World Intellect Prop 15(1):1–25

Favale M, McDonald N, Faily S, Gatizidis C (2016) Human aspects of digital rights management: the perspective of content developers. SCRIPTe d 13:289. https://doi.org/10.2966/scr1.130316.289

Felten EW (2003) A sceptical view of DRM and fair use. Commun ACM 46:56–59

Felten E (2018) Blockchain: what is it good for? https://freedom-to-tinker.com/2018/02/26/bloc. Accessed 3 April 2018

Ferrari L (2006) L’incerto cammino della tutela giuridica delle misure tecnologiche di protezione del diritto d’autore: recenti orientamenti in materia di modifica di console per videogiochi (the troublesome path of the legal protection of the copyright anticircumvention measures: recent trends with regard to the alteration of videogames consoles). Diritto dell’Internet, p 269

Finck M (2018) Blockchain regulation and governance in Europe. Cambridge University Press, Cambridge

Fitzner J (2011) Von Digital-Rights-Management zu Content Identification. Nomos, Munich
Fitzpatrick S (2000) Copyright imbalance: US and Australian responses to the WIPO Digital Copyright Treaty. Eur Intell Prop Rev 22:214–228

Geiger C, Frosio G, Bulayenko O (2018) The exception for text and data mining (TDM) in the proposed Directive on Copyright in the Digital Single Market – legal aspects. In-Depth Analysis, Brussels. https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/604941/IPOL_IDA(2018)604941_EN.pdf. Accessed 12 Nov 2018

Geiger C (ed) (2015) Research handbook on human rights and intellectual property. Edwar Elgar, Cheltenham

Gervais DL (2018) The cultural role(s) of collective management organizations. Eur Intell Prop Rev 40(6):349–356

Giancaspro M (2017) Is a “smart contract” really a smart idea? Insights from a legal perspective. Comput Law Secur Rev 33:825–835

Ginsburg JC (2013) Copyright 1992–2012: The most significant development? Fordham Intell Prop Media Ent LJ 23:467–501

Goldenfein J, Leiter A (2018) A legal engineering on the blockchain: “smart contracts” as legal conduct. Jake Goldenfein and Andrea Leiter, “Legal engineering on the blockchain: ‘smart contracts’ as legal conduct”. Law and critique (Forthcoming). https://ssrn.com/abstract=3176363. Accessed 12 Nov 2018

Goldstein P (1997) Copyright and its substitutes. Wisconsin Law Rev 45:865

Goldstein P (2003) Copyright highway: the law and core of copyright from Gutenberg to the celestial jukebox. Stanford University Press, Stanford

Grigg I (1996) The Ricardian contract. http://iang.org/papers/ricardian_contract.html. Accessed 13 Aug 2018

Guibault L (2002) Copyright limitations and contracts. An analysis of the contract overridability of limitations on copyright. Kluwer Law International, The Hague

Halaburda H (2018) Blockchain revolution without the blockchain. https://www.bankofcanada.ca/wp-content/uploads/2018/03/san2018-5.pdf. Accessed 13 Aug 2018

Heap I (2017) Blockchain could help musicians make money again. Harvard Business Review. https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again. Accessed 9 Nov 2018

Hess D (2015) Managing digital rights with rights expression languages. J Digit Med Manag 4(1):21–34

Hilty RM (2005) Five lessons about copyright in the information society: reaction of the scientific community to over-protection and what policy makers should learn. J Copyright Soc’y USA 53:103–138

Hilty RM, Nérisson S (2012) Balancing copyright a survey of national approaches. Springer, Berlin

Hilty RM (2016) Exhaustion in the digital age. In: Calboli I, Lee E (eds) Research handbook on intellectual property exhaustion and parallel imports. Edward Elgar Publ, Cheltenham

Hilty RM (2018) IP and private ordering. In: Pila J, Dreyfuss R (eds) The Oxford handbook of intellectual property law. Oxford University Press, Oxford, pp 10–47

Hilty RM, Moscon V (2018) Permitted uses in copyright law – is there need for an international instrument? In: Sun H, Balganesh S, Ng-Loy WL (eds) Comparative aspects of limitations and exceptions in copyright law. Cambridge University Press, Cambridge

Hohmann A (2016) Rights expression languages in libraries. https://hb.diva-portal.org/smash/get/diva2:970467/FULLTEXT01.pdf. Accessed 10 Oct 2018

Holden R, Malani A (2017) Can blockchain solve the holdup problem in contracts? https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3093879. Accessed 13 Aug 2018

Howell M (2005) The misapplication of the DMCA to the aftermarket. BUJ Sci Tech L 11:128–154

Hughes J (2016) Motion pictures, markets, and copylocks. George Mason Law Rev 23. Loyola Law School, Los Angeles Legal Studies Research Paper No. 2016-10. https://ssrn.com/abstract=2758830. Accessed 2 Nov 2018

Hugenholtz PB, Guibault L, Westkamp G et al. (2007) Study on the implementation and effect in Member States’ laws of Directive 2001/29/EC. Report to the European Commission, DG Internal Market. University of Amsterdam, IVIR, Amsterdam

Idelberger F et al (2016) Evaluation of logic-based smart contracts for blockchain systems. In: Alferes JJ et al (eds) Rule technologies. Research, tools, and applications. Springer, Berlin

Ito K, O’Dair M (2018) A critical examination of the application of blockchain technology for intellectual property management. In: Treiblmaier H, Beck R (eds) Business transformation through blockchain, vol 2. Palgrave. http://eprints.mdx.ac.uk/25167/ (forthcoming in 2019)

Kiviati TI (2015) Beyond bitcoin: issues in regulating blockchain transactions. Duke Law J 65:605–608
Rosenblatt B, Dykstra G (2003) Integrating content management with digital rights management: 
imperatives and opportunities for digital content lifecycles. Giant Steps, New York 
Samuleson P (1999) Intellectual property and the digital economy: why the anti-circumvention 
regulations need to be revised. Berkeley Technol Law J 14:504–566 
Samuelson P (2016) Freedom to tinker. In: Harhoff D, Lakhani K (eds) Revolutionizing innovation: users, 
communities, and open innovation. MIT Press, Cambridge 
Savelyev A (2018) Copyright in the blockchain era: promises and challenges. Comput Law Secur Rev 
34:550–561 
Sentfleben M (2016) WIPO Copyright Treaty. In: Dreier T, Hugenholtz PB (eds) Concise European 
copyright law. Kluwer Law International, The Hague, pp 93–139 
Silver J (2016) Blockchain or the chaingang? Challenges, opportunities and hype: the music industry and 
blockchain technologies, CREATe Working Paper. https://www.create.ac.uk/publications/ 
blockchain-or-the-chaingang-challenges-opportunities-and-hype-the-music-industry-and-
blockchain-technologies/. Accessed 25 Oct 2018 
Stefik M (1997) Shifting the possible: How digital property rights challenge US to rethink digital 
publishing. Berkeley Technol LJ 12:137–159 
Szabo N (1996) Smart contracts: building blocks for digital markets. http://www.fon.hum.uva.nl/rob/
Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/
smart_contracts_2.html. Accessed 13 Aug 2018 
Tresise A et al. (2018) What blockchain can and can’t do for copyright. https://papers.ssrn.com/sol3/
papers.cfm?abstract_id=3227381. Accessed 8 Nov 2018 
von Gompel S (2013) Copyright formalities in the internet age: filters of protection or facilitators of 
licensing. Berkeley Technol LJ 28:1425 
von Lohmann F (2010) Unintended consequences: twelve years under the DMCA https://www.eff.org/
wp/unintended-consequences-under-dmca. Accessed 9 Oct 2018 
Winner L (1986) The whale and the reactor. University of Chicago Press, Chicago, pp 19–39 
Yermack D (2017) Corporate governance and blockchains. Rev Finance 21:7–31 
Zeilinger M (2016) Digital art as “monetised graphics”: enforcing intellectual property on the 
blockchain. Philos Technol. https://doi.org/10.1007/s13347-016-0243-1

International Agreements

TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh 
Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 
1197 (1994)
The Berne Convention for the Protection of Literary and Artistic Works, opened for signature 9 
September 1886, 1161 UNTS 30 (entered into force 5 December 1887)

Official Acts

H.R. REP. No. 105–551, at 24 (1998)
DMCA Pub. L. No. 105–304, 112 Stat. 2860, 1998

Cases

Inc. v. GameMasters, 87 F. Supp. 2d 976 (N. D. Cal. 1999)
Stevens v. Kabushiki Kaisha Sony Computer Entertainment, HCA 58 (2005)
UK v. Kabushiki Kaisha Sony Computer Entertainment v. Ball, EWHC 1738 (2004)