

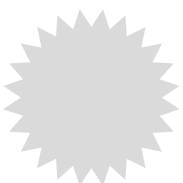


4iP Council
Research Award Winner 2018
Second Place

2

Blockchain and Copyright Issues

by Maximilian Kiemle
LL.M. student at KU Leuven in Belgium.





Rigorous empirical
research on
intellectual property

4iP Council is a European research council dedicated to developing high quality academic insight and empirical evidence on topics related to intellectual property and innovation. Our research is multi-industry, cross sector and technology focused. We work with academia, policy makers and regulators to facilitate a deeper understanding of the invention process and of technology investment decision-making.

www.4ipcouncil.com

Suggested citation

Kiemle, M. Blockchain and Copyright Issues. (January 2019).
4iP Council.

Blockchain and Copyright Issues

Table of Contents

1. Summary.....	- 1 -
2. Blockchain and copyright.....	- 1 -
2.1 Immutable ownership chains.....	- 1 -
2.1.1 Pre-blockchain situation: Various registry systems.....	- 1 -
2.1.2 The promise: Safeguarding authorship and ownership.....	- 2 -
2.1.3 The conflict: Liability for inaccurate data input.....	- 2 -
2.1.4 Potential solutions.....	- 3 -
2.1.5 Summary and outlook.....	- 4 -
2.2 Smart royalty transactions.....	- 5 -
2.2.1 Pre-blockchain situation: The value gap.....	- 5 -
2.2.2 The promise: Fair (=more) compensation.....	- 5 -
2.2.3 The conflict: Legal reversibility of Smart Contracts.....	- 6 -
2.2.4 Potential solutions.....	- 8 -
2.2.5 Summary and outlook.....	- 9 -
2.3 Higher degree of anonymity.....	- 9 -
2.3.1 Pre-blockchain situation: Anonymity to some degree.....	- 9 -
2.3.2 The promise: Absolute anonymity within the system.....	- 10 -
2.3.3 The conflict: Country of origin pursuant to art. 5 Berne Convention.....	- 11 -
2.3.4 Potential solutions.....	- 13 -
2.3.5 Summary and outlook.....	- 14 -

1. Summary

The three technical aspects of copyright blockchains reviewed are **(1) immutable ownership chains**, **(2) smart royalty transactions** and the **(3) higher degree of anonymity**. By analysing these three aspects, the research focuses on the legal applicability of those features to copyrights, rather than on their technical implementation.

A closer look at current use-cases of blockchain-based copyright registries reveals a general ignorance by companies using them of potential copyright issues. Many business whitepapers, their terms and conditions focus on the technology's benefits while leaving aside details of its implementation. Merely recognising the potential problems that blockchain applications might face would be a major step forward in finding potential solutions. Hence, future copyright registers should be developed in an open manner and include the possibility of altering the code, taking into account potential legal obligations in, while leaving 'backdoors' or subsequent changes to software developers. Companies should be open to address copyright issues and not bar the way to potential solution by implementing an immutable technology.

From a legal perspective, altering the blockchain in compliance with current laws may seem the easiest and most evident approach, but the inherent nature of blockchain inhibits simple alterations. On the one hand, a public and permissionless blockchain cannot be restricted *ex post* without ceasing to be permissionless and public. Subsequent changes must therefore be anticipated by the initial code. By allowing *ex post* modifications, permissioned blockchains undermine several of the technology's selling points such as immutability, disintermediation, anonymity and transparency. Moreover, the nature and reputation of the authority assigned with the power to modify the code might seriously affect the blockchain's appeal, given that "a centralized database is only as trusted as the entity that controls the database".¹ As a result, developers of blockchain-based copyright registries have to carefully assess the advantages and disadvantages of public/private and permissioned/permissionless systems before opting for one of these solutions.

¹ H. MAZOR, *Can Blockchain Technology Solve Copyright Attribution Challenges of Digital Work?*, IP Watchdog, February 2, 2018, cf. www.ipwatchdog.com/2018/02/02/blockchain-technology-solve-copyright-attribution-digital-work/id=93161/.

Adapting copyright laws might be a viable, but often impracticable solution to resolving conflicts between blockchain technology and copyright frameworks. Taking into account the juxtaposition of one technology and hundreds of different national and international copyright frameworks, it is often easier for a company to adjust the technology than to address fragmented legislation (especially as a globally harmonized copyright framework might be desirable it is currently a pipe dream). Nevertheless, copyright law reform should occur where the issues are not exclusively due to new technology but rather general underlying conflicts of the legal framework. Hence, the rise of blockchain makes a reform of the Berne Convention with regard to the author's anonymity more pressing.

The looming conflicts with copyright laws will not impede blockchain technology's popularity and companies increasingly offering blockchain-based copyright registries. As legislators are unlikely to tackle the copyright challenges through new legislation *ex ante*, the widespread application and use of blockchain technology is likely to lead to non-compliance decisions by national authorities and courts that will provide precedents for business and direction for legislative reforms. In the meantime, users of blockchain-based copyright registries have to live with substantial legal uncertainty.

2. Blockchain and copyright

2.1 Immutable ownership chains

2.1.1 Pre-blockchain situation: Various registry systems

Currently, copyright registries around the world are not active at the global level nor harmonised, but restricted to their territorial jurisdiction. Art. 5 (2) of the Berne Convention² prohibits the imposition of formalities on foreign authors for the enjoyment and exertion of their rights in that territory. Thus, the Bern Convention does not require a national registration for copyrights for the right to take legal effect, unless such an obligation is set out by the national law *for domestic authors*.³ Some national laws do create public copyright registries. Those registries can be divided by their legal effects in purely voluntary registries and quasi-mandatory registries. The nature of registries varies depending on the national approach. In Germany, for example, no public registry exists to register a work for protection.⁴ On the other hand, the Spanish government provides a public registry, the use of which is voluntary but once a work is registered the entry yields a presumption of existence, authorship and date of creation.⁵ Finally, the U.S. established a quasi-mandatory system. Registration is not required in order to enjoy copyright protection, but is *conditio sine qua non* for domestic copyright holders if they wish to start copyright infringement proceedings before a federal court.⁶

Apart from public registries, a variety of private companies offer copyright databanks. Registration with those private companies does not bear any immediate legal effect, but ensures a higher degree of probative value due to third party data storage and time-stamps.⁷ As a result of the often nation-specific public and small-sized private registries, copyrighted content is often scattered across various third-party databases.

² Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979).

³ C. J. SPRIGMAN, *Berne's Vanishing Ban on Formalities*, 28 Berkeley Tech L. J., 2013 p. 1566.

⁴ "Registering a work for protection is neither required nor possible", Deutsches Patent- und Markenamt, cf. www.dpma.de/dpma/wir_ueber_uns/weitere_aufgaben/verwertungsges_urheberrecht/index.html. Under German law, copyright registries only exist with regard to out-of-print and anonymous/pseudonymous works exist, cf. § 13e and § 138 Urheberrechtsgesetz.

⁵ Cf. Real Decreto 281/2003, de 7 de marzo, por el que se aprueba el Reglamento del Registro General de la Propiedad Intelectual, www.boe.es/buscar/doc.php?id=BOE-A-2003-6247; cf. for the corresponding Argentinean registry: Argentinean Ministry of Justice: www.jus.gob.ar/derecho-de-autor/beneficios-del-registro.aspx.

⁶ 17 United States Code § 411.

⁷ P. DE FILIPPI, G. MCMULLEN et al., *How Blockchains can Support, Complement or Supplement Intellectual Property*, COALA Report, Working Draft, p. 4.

To conclude, there is no fully mandatory registry in place anywhere in the world, let alone a harmonised global public system. And there is not one single market player among the private companies that pools all or just a substantial part of the world's copyright data. This lack of transparency makes it difficult and burdensome to assess whether a work, such as an image found online, is copyright protected or not. Consequently, either potential users refrain from using the image or risk infringing the copyright. In both cases the right holders may be deprived of their fair compensation.

2.1.2 The promise: Safeguarding authorship and ownership

Blockchain technology could be part of the solution to this lack of transparency by establishing an easily accessible – and at the same time reliable – copyright database. The above-mentioned characteristics of blockchains, i.e. transparency, decentralization and immutability, would ensure that copyrighted works, their authors, owners and other right holders, are known to potential users of the protected works. Private companies have already developed blockchain-based copyright databases. One example is *ascribe*, a company that specialises in enabling the upload of protected works to “create a permanent and unbreakable link” between the right holders and their works.⁸ Users of *ascribe*'s service can then share, (sub)license and transfer their works/rights and trace (potentially) infringing uses of their works online.⁹ Works uploaded into such blockchains will be time-stamped, i.e. an immutable stamp will indicate the date and time of the action.

2.1.3 The conflict: Liability for inaccurate data input

One of the highly acclaimed features of blockchains, the immutability of its data, yet this constitutes one of its main drawbacks. The blockchain creates a new narrative, parallel to the “off-chain” world. Within the blockchain, the system is immune to alteration, tampering and falsification. Human errors, leaks and intentional fraud occur at the interfaces between blockchain and off-chain world.¹⁰ One of those vulnerable situations is the input of data (garbage in/garbage out idea).¹¹ How should and how could the blockchain respond to the input of copyright data that is false from the beginning or to a situation where the off-chain

⁸ Cf. www.ascribe.io.

⁹ *Ibidem*.

¹⁰ Cf. for the famous Mt. Gox (a Japanese bitcoin exchange) and other hacks: J.H. PARK, J.H. PARK, *Blockchain Security in Cloud Computing: Use Cases, Challenges and Solutions*, Symmetry-Basel, 2017 Aug, Vol.9(8).

¹¹ A. WALCH, *Blockchain's Treacherous Vocabulary: One More Challenge for Regulators*, Journal of Internet Law, New York, Vol. 21, Number 2 (August 2017), p. 10.

data does not correlate with the data on the blockchain anymore, e.g. due to an off-chain change of legislation or court ruling? And what are the legal consequences? Another structural handicap of blockchain's immutable ownership chains is the 'all-or-nothing' approach. The blockchain can barely react to transfers of ownership that occur off-chain. Right holders must choose either to conclude all ownership transfers on the chain or continue to transfer rights off-chain. This makes the system highly inflexible and limits the right holders' freedom to act and could enable infringement. If right holders nevertheless engage in a two-pronged approach and transfer rights both off and on the chain, the data on the blockchain may become inaccurate.

All copyright regimes grant right holders economic rights and to some degree moral rights (due to art. 6bis Berne Convention). Depending on individual rights and the applicable national legislation, the right holder has the right to prohibit (or defend) and the right to authorize certain acts with regard to the protected work. Those rights, *inter alia*, include the right to prohibit unauthorised use of copyrighted works.¹² Most of the cases in which data on a copyright blockchain might become inaccurate would include false or outdated attribution of rights. Due to inaccuracy at the time of the input or later off-chain developments third parties may have acquired rights that were not updated on the chain. To ensure that the falsely attributed right holder will not further transfer rights or content via the blockchain database, the actual right holder could enforce his rights, e.g. by starting an injunction against the "blockchain right holder". EU-wide, the possibility of such national injunctions is harmonised through the Enforcement Directive.¹³

When looking at current implementations of copyright blockchains, it becomes evident that companies like *ascribe* are well aware of the possibility of inaccurate data input by users. The approach *ascribe* takes is to limit their own liability in their Terms of Service by stating that *ascribe* does not verify the accuracy of the data.¹⁴

2.1.4 Potential solutions

The following example demonstrates the abovementioned conflict and potential solutions in practice: What if A uploads work X to the blockchain, claiming to be both the author and the

¹² J. PILA, P. TORREMANS, *European Intellectual Property Law*, Oxford University Press 2016, p. 298.

¹³ Art. 11 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

¹⁴ 4. The Services, Limitation of Liability, cf. www.ascribe.io/terms.

owner of the work, while in the off-chain reality B is author and sole owner of work X? The first solution requires the rectification by a blockchain administrator and the second requires the off-chain enforcement, in order to ultimately coerce A to rectify the inaccurate data on the blockchain.¹⁵ The first solution is only available where the permissioned blockchain, includes an authority to modify the data exists (i.e. the blockchain is less 'revolutionary'). The second solution is only feasible if the particular blockchain code allows the alteration of data by the user who first uploaded it. That is by no means self-evident as the immutability of blockchains often goes far beyond the influence of the people who once were responsible for the input.¹⁶ But even if the code was to allow such an alteration by A, it would require the authorities to identify A in the first place. Identification, however, would be nearly impossible in a permissionless blockchain due to the anonymity of its users.

Instead of adapting the law or reversing to permissioned blockchains administered by a single authority, one option is to allow several trustworthy entities or individuals (as verified users of the blockchain) to validate authorship and ownership of the works on the blockchain. These verified users could be museums, researchers, galleries and universities with a special status on the blockchain.¹⁷ Yet the added value of these authorities is limited to their expertise which will not include works by publicly unknown artists or one-time copyright authors. And there are more flaws to this solution. Firstly, those verified users would render the blockchain less open and less democratic. Secondly, it would require one singular powerful authority to define who is to be verified and who is not. Whereas the latter could be overcome by a consensus process, the blockchain would be a less open one either way.

2.1.5 Summary and outlook

A closer look at the promise of safeguarding authorship and ownership through immutable and transparent records reveals frictions between the technical possibilities and the legal realities. Blockchain-based copyright registries will face obstacles when it comes to enforcement with regard to inaccurate data. In order to tackle this issue, blockchains will

¹⁵ A. SAVELYEV, *Copyright in the blockchain era: Promises and challenges*, Computer Law & Security Review 34 (2018), p. 557.

¹⁶ A. LEWIS, *A Gentle Introduction to Immutability of Blockchains*, Bits on Blocks, February 29, 2016, <https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/>.

¹⁷ P. DE FILIPPI, G. MCMULLEN et al., *How Blockchains can Support, Complement or Supplement Intellectual Property*, COALA Report, Working Draft, p. 5.

have to adapt to comply with the current laws, given that laws will not adapt in time to the new technology.

As the *ascribe* case shows, blockchain companies follow this path by heavily restricting the openness and immutability of blockchains. Interestingly enough, *ascribe* seeks to meet current legal requirements not (only) by integrating restrictions into the code but by relying on a second tier in the “off-chain” world; the Terms of Service. Current and future business models might therefore follow *ascribe*’s example and introduce a second mandatory component. By doing so, they are in a better position to address potential problems *ex ante* and retain the possibility to react to claims of inaccurate data. Nevertheless, if those limitations are not embedded in the blockchain code itself, the data would remain on the blockchain regardless of any efforts made off-chain. Once a central authority such as a company or organisation reserves the right to correct the blockchain, the blockchain qualifies as a private and not as a public system.

2.2 Smart royalty transactions

2.2.1 Pre-blockchain situation: The value gap

So far traditional licensing instruments, like individual licensing, have not been effective in dealing with the use of copyrighted works in an all-connected digital environment. Unlike analogue copies, the reproduction of digital content hardly entails any costs. Private and professional users both have the incentive and means to use copyrighted works on the internet without asking for authorization. Even users acting in good faith are often unaware of copyright protection, unable to identify whether a work is protected and unable to seek authorisation in case of protection. In addition, the identification process makes the transaction fairly costly and potential buyers may refrain from using the work.¹⁸ Hence, right owners are deprived of their license fees. The so-called value gap between unauthorised use and fair compensation has led to calls for greater intervention by legislators.¹⁹

¹⁸ P. GOLDSTEIN, *Future Platforms for Copyright Licensing*, IIC - International Review of Intellectual Property and Competition Law, 2015, Vol. 46, Issue 2, p. 153.

¹⁹ J. PILA, P. TORREMAN, *European Intellectual Property Law*, Oxford University Press 2016, p. 257.

2.2.2 The promise: Fair (=more) compensation

Copyright blockchains address the problem by approaching it from a more technical than legal angle. Companies offering copyright blockchains promise fair compensation in two ways: Firstly, right holders will receive a greater share in royalties, because the blockchain renders costly intermediaries superfluous. Secondly, blockchains promise an increase of authorised uses due to a simplified, easily accessible and automatic licensing system, built on smart contracts. Smart contracts allow a high degree of billing granularity. Micropayments of fractions of cents can therefore be concluded precisely and efficiently.²⁰ That mechanism allows authors to receive compensation for transient and temporary use of their works which they otherwise would not have got. A relevant use-case, soon to be implemented, is a blockchain-based video on demand platform called StreamSpace.²¹ The platform intends to act as a “marketplace” for filmmakers who can distribute their works directly to customers. According to the developers, filmmakers will be enabled to set their own individual prices and enjoy the security of a decentralised storage system,²² whereas consumers will have access to unique works that would otherwise not have found their way to the end-consumer.²³

2.2.3 The conflict: Legal reversibility of Smart Contracts

One of the most important instruments for right holders to market their works is the issuing of licenses. Licenses form a unique intersection between mandatory copyright laws and the freedom of contracts.²⁴ The contracting parties are free to determine the territorial, personal, temporal and material scope of the licensing agreement, exclusivity or sublicenses. Licensing agreements, like all contracts, have different provisions to deal with breach by one of the parties or a material change of facts and circumstances. One way is to include explicit provisions for the specific triggering event and the corresponding legal consequence. Another way is a renegotiation clause. And a third way are vague legal terms like “reasonable”, “fair” and “due cause”. These widely used legal terms leave room for

²⁰ S. YASSAMI, N. DREGO, I. SERGEEV, T. JULIAN, D. HARDING, B. S. SRINIVASAN, *True Micropayments With Bitcoin*, Medium Corporation, 2016, cf. <https://medium.com/@earndotcom/true-micropayments-with-bitcoin-e64fec23ffd8>.

²¹ To be launched publicly in the third quarter of 2018, cf. www.stream.space/faq.

²² What is Streamspace? and Our Community, cf. www.stream.space.

²³ StreamSpace Whitepaper, p. 5, cf. www.stream.space/pdf/StreamSpace_White_Paper.pdf.

²⁴ B.J. ARD, *Notice and Remedies in Copyright Licensing*, Missouri Law Review, 2015, Vol.80(2), p. 313.

interpretation. Ultimately, courts may need to intervene in cases of diverging interpretations between the parties. The advantage of the vagueness lies in their flexibility, which can catch a broad spectrum of unforeseen scenarios.

Although the term “smart contracts” appears to be rather straightforward, the legal classification of smart contracts is far from simple. A widely used saying is that “smart contracts are neither smart nor contracts”.²⁵ Smart contracts lack the offer and/or acceptance criteria, essential to qualify as a contract under most jurisdictions. Smart contracts are rather a technical mode to execute “actual contracts”, i.e. contracts as defined by law.²⁶ Smart contracts that are part of a blockchain cannot be easily altered by the individual users. Their execution follows the initial code. In order to modify or reverse a smart contract, the triggering event for the modification and its consequence, e.g. termination or extension, must have been anticipated by the code. Although the code might foresee an extensive spectrum of potential future conflicts, it will be not be able to anticipate each and every facet of a multifarious legal reality.²⁷ Some contracts might even depend on external factors from the outset, such as insurances requiring data about real-life events of damages. These external factors have either to be anticipated or must be dynamically synchronised with the smart contract.²⁸

But even if a real-life event was anticipated by the code, the code itself could be subject to human error. Drafting codes for smart contracts will require both extensive legal experience and professional programming skills. Hence, codes of smart contracts are susceptible to include bugs due to human error or incomplete information.²⁹ The open question of liability in such cases adds to the legal uncertainty.³⁰ Moreover, smart contracts do not allow the parties to resolve the dispute informally.³¹ Off-chain, parties using contracts in the traditional

²⁵ G. GOVERNATORI, F. IDELBERGER, Z. MILOSEVIC et al., *On legal contracts, imperative and declarative smart contracts, and blockchain systems*, Artif. Intell. Law (2018), p. 8; R. O'SHIELDS, *Smart Contracts: Legal Agreements for the Blockchain*, 21. N.C. Banking Inst. 177, 2017, p. 178.

²⁶ É. BARBRY, *Smart contracts... Aspects juridiques*, Annales des Mines - Réalités industrielles, 19 July 2017, Issue 3, p. 77.

²⁷ G. GOVERNATORI, F. IDELBERGER, Z. MILOSEVIC et al., *On legal contracts, imperative and declarative smart contracts, and blockchain systems*, Artif. Intell. Law (2018), p. 26.

²⁸ M. GIANCASPRO, *Is a “smart contract” really a smart idea? Insights from a legal perspective*, Computer Law & Security Review 33, 2017, p 833.

²⁹ W. A. KAAL, C. CALCATERRA, *Crypto Transaction Dispute Resolution*, The Business Lawyer ; Chicago Vol. 73 (1), p. 131.

³⁰ M. GIANCASPRO, *Is a “smart contract” really a smart idea? Insights from a legal perspective*, Computer Law & Security Review 33, 2017, p 829.

³¹ J. M. SKLAROFF, *Smart Contracts and the Cost of Inflexibility*, University of Pennsylvania, Law Review, Volume 166, Issue 1, 2017, p. 277.

sense might agree to forego the legal consequences initially intended in a contract and come to an amicable agreement. Based on the parties' current consensus and common sense, these informal dispute settlements often lead to a lasting legal agreement. On-chain, however, smart contracts do not allow such informal settlements not anticipated by the code.

StreamSpace explains on its website how the company intends to distribute payments through smart contracts. StreamSpace users will have to pay a fee for watching or permanently downloading films. A certain amount of that fee goes to the platform provider. If necessary, the remaining payment fees can be split and go to different right holders.³² In the case of StreamSpace licenses are only issued to end-users. Hence there is no need or demand for complex license agreements that would include specific clauses like sublicensing. Nevertheless, even the code of these basic agreements might not predict all eventualities. As a fairly trite example, a power outage could hinder the user to watch the film he just rented for no more than 24 hours. Liability for such force majeure events may be governed by the applicable national law. What if the user wants his money back or an additional 24 hours to watch the film? There is a chance that the right holder is indeed obliged to refund the user under the applicable law. Open questions remain as to how the initial transfer, based on smart contracts, can be technically reversed. Moreover, in case that the transfer is flawed due to an initial error within the code, reversing the smart contract code is simply not possible without the onerous step of reversing the entire blockchain.³³

2.2.4 Potential solutions

As of now, companies like StreamSpace do not provide solutions to these potential issues. It is doubtful from the above that future solutions can be solely based on smart contracts. Unlike legal contracts, the lack of flexibility of smart contracts does not allow those automatic execution modes to include vague terms or interpret unforeseen scenarios. For this reason, blockchain smart contracts may be highly problematic. Hence, companies should engage in developing self-executing software that respects the legal realities of today and allows smart contracts to be managed from the parties after the first execution.

³² StreamSpace Whitepaper, p. 15, cf. www.stream.space/pdf/StreamSpace_White_Paper.pdf.

³³ L. LUU, D.-H. CHU, H. OLICKEL, P. SAXENA and A. HOBOR, *Making Smart Contracts Smarter*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (24–28 October 2016), Vienna, p. 255.

Following a different approach, the legislator could adapt the current laws. However, adapting the law might not be a preferable option for several reasons: Whereas blockchains are designed to act globally, copyright laws are still predominantly confined to a national territory. As a result, a lot of traditional legal frameworks would have to be revised. In addition, the legal tradition of a highly flexible law of contracts derives from a well-founded rationale. The flexibility of contractual law mirrors the complexity of a legal reality full of unforeseeable scenarios. The success of today's legal frameworks lies within the liaison between statutory law and its interpretation by the parties and courts. A blockchain not open to interpretation would simply ignore these achievements.

2.2.5 Summary and outlook

The processing of royalty transactions based on blockchain and smart contracts has to overcome various pitfalls. In particular, the designer of a blockchain-based copyright database must ensure a high degree of flexibility when it comes to (legal) contracts, their subject matter and their reversibility.

As shown above, StreamSpace and other examples of royalty transaction platforms have not taken these issues into consideration. To avoid systemic failures, they should adapt the flexibility and the scope of their application according to the relevant laws. Smart royalty transactions must be technically reversible by design in order to prove their long-term effectiveness.

2.3 Higher degree of anonymity

2.3.1 Pre-blockchain situation: Anonymity to some degree

Starting with two definitions, an anonymous work is of unknown and unidentifiable authorship, whereas a pseudonymous work is published under a fictitious name.³⁴ If the author's identity behind the pseudonym is not commonly known, the situation of a pseudonymous work is similar to that of an anonymous work.³⁵ The only difference is that the general public can make a link between the works an unknown author has published under the same pseudonym. Due to the similarity of anonymous and "non-identifiable"

³⁴ Definitions of anonymous and pseudonymous in Merriam Webster, cf.

www.merriam-webster.com/dictionary/anonymous; www.merriam-webster.com/dictionary/pseudonymous.

³⁵ For this reason, the Berne Convention treats anonymous and not-identifiable pseudonymous works equally, cf. art. 15 (1) and (3).

pseudonymous works, the use of the word “anonymous” in the following refers to both cases.

Anonymous works should not be confused with orphan works. There is no explicit legal delineation between orphan works and anonymous works. Orphan works are works for which no right holder could have been identified or located. The EU has harmonised the notion by adopting the Orphan Works Directive.³⁶ The Directive does not provide a definition of anonymous works. However, the “Directive shall be without prejudice to national provisions on anonymous or pseudonymous works”.³⁷ The Directive aims at making works available to the public where the right holders’ prior consent cannot be obtained. Following the Directive’s rationale, the delineation must be made where an author stays anonymous (unidentified and untraceable) but can be contacted. Contact between the author and the consumers could be established by setting up a company, a website or engaging intermediaries. Against this background, such a case would not qualify as an orphan work under the Directive.

Copyright frameworks recognise the need for protection of anonymous authors. The Berne Convention explicitly mentions anonymous works in connection with the term of protection. Since the term of protection cannot be based on the anonymous author’s lifetime, the protection “shall expire fifty years after the work has been lawfully made available to the public”.³⁸ The corresponding EU provision grants the anonymous work 70 years of protection after the lawfully making available to the public.³⁹ In addition, the Berne Convention stipulates a presumption that confers the enforcement of the anonymous author’s right on the publisher.⁴⁰ Corresponding provisions exist not in EU but in some national laws.⁴¹ Moreover, several national laws qualify the right to remain anonymous explicitly as a moral right.⁴²

³⁶ Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works.

³⁷ Art. 2 (5) Orphan Works Directive.

³⁸ Art. 7 (3) Berne Convention.

³⁹ Art. 1 (3) Term Directive, i.e. Directive 2006/116/EC of the European Parliament and the Council of 12 December 2006 on the term of protection of copyright and certain related rights.

⁴⁰ Art. 15 (3) Berne Convention.

⁴¹ **Spain:** Art. 6 (2) Ley de propiedad intelectual; **Germany:** § 10 (2) Urheberrechtsgesetz.

⁴² **Canada:** Copyright Act - R.S.C., 1985, c. C-42 (Section 14.1 (1)); **Chile:** Art. 14 (5) Ley N° 17.336; **Germany:** § 13 S. 2 Urheberrechtsgesetz.

2.3.2 The promise: Absolute anonymity within the system

Blockchain technology's promise of anonymity is one of its key selling points.⁴³ Blockchain users can create new identities on the chain and act under this identity within the blockchain-based system. The blockchain identity thus serves as non-identifiable pseudonym and does not provide an anonymous space *sensu stricto*.⁴⁴ Nonetheless, a permissionless blockchain allows its user to withhold all information that could potentially link the user's blockchain identity with his off-chain identity. For this reason, it can only be estimated how many people actually use blockchain-based applications such as Bitcoin by looking at the number of existing "wallets".⁴⁵ The use of blockchain-based cryptocurrency excludes the need to store personal data with intermediaries and the buyer may not even disclose his identity vis-à-vis the vendor.⁴⁶

On a copyright blockchain, authors could time-stamp their works, prove authorship and ownership and exercise their economic rights using nothing but their on-chain pseudonym. The following sub-chapters will look at the practical implementation of the aforementioned features, namely at Creativechain, a blockchain-based project.⁴⁷ Creativechain provides a platform for the certification of authorship and licensing of digital content. Authors can choose between remaining anonymous and disclosing their identity. Interestingly enough, the designers of Creativechain have taken into account the copyright law perspective of their project. Via the platform, users can ask copyright lawyers for advice and assistance. Furthermore, the platform uses its own cryptocurrency "Creativecoin" that can be used anonymously, thus making "Creativecoin a perfect currency to register contents anonymously".⁴⁸

⁴³ G. ORUM HERNÁNDEZ, *With Contract Automation, Ambition Doesn't Always Align with Reality*, Legaltech News, March 30, 2017.

⁴⁴ T. BELL, *Copyrights, Privacy, and the Blockchain*, Ohio Northern University Law Review, 39th Annual Symposium Articles, p. 464.

⁴⁵ A. LIELACHER, *How Many People Use Bitcoin?*, www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/.

⁴⁶ J. FAIRFIELD, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, Washington and Lee Law Review Online, Vol. 71 (2), p. 46.

⁴⁷ Cf. www.creativechain.org/project/.

⁴⁸ Creativechain Whitepaper, p. 4, 5 and 8, cf.

<https://creativechain.org/wp-content/uploads/2017/03/Whitepaper-Creativechain-1.2.pdf>.

2.3.3 The conflict: Country of origin pursuant to art. 5 Berne Convention

The notion of country of origin is of high relevance under the Berne Convention. Art. 5 of the Berne Convention guarantees rights depending on the country of origin. In addition, the term of protection shall – in principle – not exceed the term fixed in the country of origin.⁴⁹ Furthermore, the Convention applies only to works for which protection in their country of origin has not been expired at the moment of the Convention's coming into force.⁵⁰ Art. 5 (4) defines the notion of country of origin, stating that when published simultaneously in various countries of the Berne Union, the country which grants the shortest term of protection should be considered the country of origin.⁵¹ Since the internet, as well as the blockchain, enables users from all the countries forming part of the Berne Union simultaneously to access the works, the country with the worldwide shortest protection would be the country for all the works first published online.⁵² However, many Berne Union members have the same minimum protection term of the author's lifetime, plus 50 years. Hence, following this approach does not significantly narrow down the applicable protection.⁵³ The Berne Convention raises more questions than it provides guidance. It is not even clear whether the notion of publishing within the meaning of Art. 3 (3) Berne Convention covers the publication in digital form. The Berne Convention speaks of "manufacture of the copies". This provision originates from the time when copyright laws intended to regulate the printing press.⁵⁴ Because of the wording and the absurdity arising from simultaneous digital publications falling under the notion of publishing, i.e. the vast number of country of origins, legal experts tend to exclude purely online or digital publication from the scope of Art. 3 (3) Berne Convention.⁵⁵ If a work is not published within

⁴⁹ Art. 7 (8) Berne Convention.

⁵⁰ Art. 18 (1) Berne Convention.

⁵¹ Art. 5 (4) lit. a Berne Convention.

⁵² Cf. with regard to works on the internet D. THUM, *Internationalprivatrechtliche Aspekte der Verwertung urheberrechtlich geschützter Werke im Internet*, GRUR Int 2001, p. 12 et seq.

⁵³ J. GINSBURG, *When a Work Debuts on the Internet, What Is its 'Country of Origin' – Part II*, Column, The Media institute, 2012, cf. www.mediainstitute.org/2012/01/23/when-a-work-debuts-on-the-internet-what-is-its-country-of-origin-part-ii/.

⁵⁴ J. DRYDEN, *The Meaning of Publication in Canadian Copyright Law*, Intellectual Property Journal, Vol. 29 (3), 2017, p. 474 et seq.

⁵⁵ J. BLOMQUIST, M. FICSOR, Y. GENDREAU, J. GINSBURG, S. VON LEWINSKI, D. LIPSZYC, A. QUAEDVLIEG, S. RICKETSON, P. SPADA, M. WALTER, *Determination of Country of Origin When a Work is First Publicly Disclosed Over the Internet*, Report by the Country of Origin Study Group of the International Literary and Artistic Association (ALAI), 2012, p. 5; J. GINSBURG, *When a Work Debuts on the Internet, What Is its Country of Origin?*, Column, The Media institute, 2011, cf. www.mediainstitute.org/2011/08/29/when-a-work-debuts-on-the-internet-what-is-its-country-of-origin/.

the meaning of Art. 3 (3) Berne Convention or first published outside the Berne Union, the author's nationality serves as the reference point for the country of origin.⁵⁶

As mentioned above, the blockchain technology will enhance the degree of anonymity authors may use to publish their works. Under absolute anonymity on a permissionless blockchain-based copyright registry, two scenarios are conceivable. In one scenario, the work is first published within the meaning of art. 3 (3) Berne Convention. In this case, the country of origin is that of the shortest protection. As the blockchain is decentralised, simultaneous and functions globally, the situation is identical to that of publications on the internet. The aforementioned open questions in academic debate and case law⁵⁷ hold for this case too. In essence, the blockchain does not pose questions that the rise of internet did not already entail. The other scenario applies where the work is not published within the meaning of art. 3 (3) Berne Convention. Here, the country of origin follows the author's nationality. However, as user of a permissionless blockchain, the author remains anonymous. His nationality will not be known. Such a "truly anonymous" work will have no country of origin and as a consequence will not enjoy protection under the Berne Convention.⁵⁸ These truly anonymous works already existed before the advent of the blockchain technology. Again, the conflicts between the Berne Convention provisions and the blockchain with regard to the authors' anonymity are not new in terms of their nature but in terms of their scale.

The Creativechain project does not explicitly address the issue of anonymity and country of origin. In addition, the Terms of Use are rather nebulous. The text avoids referring to any specific national, international or regional regulations. The Terms, however, oblige the user to be a resident of a country where Creativechain is available.⁵⁹ Yet this provision, even if complied with, does not reveal the user's nationality. Hence, interpretation of the Terms does not entail much added value determining a country of origin.

⁵⁶ Art. 5 (4) lit. c Berne Convention.

⁵⁷ J. GINSBURG, *When a Work Debuts on the Internet, What Is its 'Country of Origin' – Part II*, Column, The Media institute, 2012, cf. www.mediainstitute.org/2012/01/23/when-a-work-debuts-on-the-internet-what-is-its-country-of-origin-part-ii/; C. DOMBKOWSKI, *Simultaneous Internet Publication and the Berne Convention*, Santa Clara High Technology Law Journal, Vol. 29 (4), 2013, p. 669 et seq.

⁵⁸ J. GINSBURG, *When a Work Debuts on the Internet, What Is its 'Country of Origin' – Part II*, Column, The Media institute, 2012, cf. www.mediainstitute.org/2012/01/23/when-a-work-debuts-on-the-internet-what-is-its-country-of-origin-part-ii/.

⁵⁹ Creativechain Terms of Use, cf. www.creativechain.org/termsofuse/.

2.3.4 Potential solutions

With regard to the country of origin conflict, an increased usage of blockchain applications would render a reform of the Berne Convention even more pressing.⁶⁰ The Convention's principle of country of origin and its points of attachments were outdated long before the evolution of blockchain. A reformed Berne Convention should take into account the digital publication of works as the norm. Recommendations have been made to interpret the current Berne Convention in a "forward-looking" way by using the nationality of the publisher within the meaning of Art. 15 (3) to determine the country of origin if the author's identity is unknown.⁶¹ However, this approach would not cover anonymous authors using the blockchain in order to make their works available to the public and thus omitting intermediaries such as publishers within the meaning of Art. 15 (3).

Safeguarding the author's anonymity, the country of protection could be defined by the server location of users who access or license the work. In this case, the privacy of the users' data should be equally protected, e.g. by only using aggregated and anonymised data. Yet this approach is only viable where a certain amount of data is being produced, i.e. a certain number of people access or license the works. Moreover, this approach might not always reflect a strong relationship between the author and the country's social, economic and legal traditions. But it is hardly feasible to respect the author's anonymity and at the same time to define a country of origin as having social, economic or legal ties with the author. A reform would have to balance both rationales. Hence, the approach of determining an anonymous author's country of origin by server location of users who access or license the work proves to be the most viable solution to this conflict.

2.3.5 Summary and outlook

A permissioned blockchain would be a solution to the country of origin issue, provided that the central authority managing the blockchain both knows the users' identities and is willing and able to disclose this information. This approach would, however, lead to a lesser degree of anonymity. And removing anonymity might be highly problematic for the privacy and

⁶⁰ Equally endorsing a reform of the Convention rather than a new "special agreement", J. DRYDEN, *The Meaning of Publication in Canadian Copyright Law*, Intellectual Property Journal, Vol. 29 (3), 2017, p. 475.

⁶¹ J. BLOMQUIST, M. FICSOR, Y. GENDREAU, J. GINSBURG, S. VON LEWINSKI, D. LIPSZYC, A. QUAEDVLIEG, S. RICKETSON, P. SPADA, M. WALTER, *Determination of Country of Origin When a Work is First Publicly Disclosed Over the Internet*, Report by the Country of Origin Study Group of the International Literary and Artistic Association (ALAI), 2012, p. 8.

potentially also for the safety of the author as there can be many cogent reasons to stay anonymous, e.g. for whistle-blowers, political dissidents or protected witnesses. Moreover, removing anonymity hinders the successful evolution of blockchain applications as it undermines the trust in this new technology.⁶² Hence, it would be more desirable to adapt current legislations, preparing them for the reality of distributed (internet) and decentralised (blockchain) anonymous works.

Whatever the technical or legal response, the enforcement issues and the problematic task of determining a country of origin form two severe obstacles for anonymous authors. In addition, anonymity entails a variety of further problems that go beyond the scope of this paper such as the liability of anonymous authors.⁶³ And with the popularity of blockchain and the rise of other digital encryption mechanisms that ensure absolute anonymity the number of conflicts will increase significantly. Nevertheless, legislators, academics and businesses should see the looming anonymity issues as an opportunity to develop new solutions.

⁶² W. A. KAAL, C. CALCATERRA, *Crypto Transaction Dispute Resolution*, The Business Lawyer ; Chicago Vol. 73 (1), p. 131.

⁶³ M. WEICHER, *[Name Withheld]: Anonymity and Its Implications*, Proceedings of the American Society for Information Science and Technology, Vol. 43 (1), 2006, p. 5.