Legal Knowledge and Information Systems
M. Palmirani (Ed.)

© 2018 The authors and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/978-1-61499-935-5-81

Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure

Ugo PAGALLO[a,1], Eleonora BASSI[b], Marco CREPALDI[a], and Massimo DURANTE[a]
[a] *University of Turin, Law School*
[b] *Politecnico of Turin, Nexa Center*

Abstract. GDPR abiding blockchain systems are feasible. Jurists, programmers, and other experts are increasingly working on this aim nowadays. Still, manifold blockchain networks functioning out there suggest a new generation of data protection issues brought about by this technology. Some of these issues will likely concern the right to erasure set up by Art. 17 of the EU data protection regulation ('GDPR'). These cases will soon be discussed before national authorities and courts, and will likely test the technical solutions explored in this paper, such as hashing-out methods, keys destruction, chameleon hash functions, and more. By taking into account matters of design and the complex architecture of blockchains, we shall distinguish between blockchains that have been thought about to expressly meet the requirements of the EU regulation, and blockchains that, for one reason or another, e.g. ante GDPR designed blockchains, trigger some sort of clash with the legal order, that is, (i) matters of principle on e.g. political decentralization; (ii) standards on security and data protection; (iii) a mix of them; and, (iv) social clash. It is still unclear how the interplay of legal regulation, technological constraints, social norms, and market interests, will end up in this context. Rulings and court orders will be instructive. It is a clash foretold, after all.

Keywords. Blockchain, chameleons hash functions, data protection, encryption, hashing-out methods, right to erasure.

1. Introduction

There is a multi-faceted parallel between current blockchain technologies and peer-to-peer ('P2P') systems, i.e. the massively distributed platforms for information storage and retrieval, which became popular in the late 1990s with the Napster case [1]. Among their features, such as tamper-proof and append-only properties, blockchains are a kind of P2P network [2]. As occurred with the spread of such distributed and decentralized systems twenty years ago [3], many claim that blockchains can strengthen social interaction to such an extent, that the creation of a libertarian cyberspace, a direct online democracy, or even a digital form of communism could be at hand [4].

There is the other side of the coin, though. Similar to the first wave of P2P networks in the 1990s and the 2000s, blockchains raise several legal issues. The DAO case, namely, a short-lived experiment that aimed to create a decentralized, directly managed crowdfunding and investment vehicle to back development projects on the Ethereum blockchain, illustrates this point with a theft of millions of dollars [5]. One of

[1] Ugo Pagallo, Law School, University of Turin, Lungo Dora Siena 100 - 10135 Torino, Italy; E-mail: ugo.pagallo@unito.it.

our main contentions will be that such legal issues of the blockchain are systemic, that is, they concern the very architecture of blockchain, as occurred with P2P technology two decades ago. What, then, was the main legal issue of these latter systems, which can help us understand the most relevant challenges triggered by the functioning and design of blockchains in the legal domain today?

After the legal misadventures of Napster—the first popular file-sharing system on the internet, which bankrupted in September 2002 after a copyright lawsuit filed by the US record industry association—the main legal issue of P2P systems revolved around whether or not this technology is "incapable of non-infringing uses." Three years later, in the 2005 *Grokster* case, the US Supreme Court's decision had to clarify to what extent technologies promoting the ease of infringing on copyrights have to be condemned, so that producers of P2P software, like Grokster and Steamcast, could be sued for "inducing copyright infringement committed by their users." In connection with the figures of the Wikipedia entry, according to which "90% of files shared on Grokster were downloaded illegally," the point of the claimants was clear: plaintiffs claimed that infringing uses of P2P technology constituted the primary aim of such systems. Although Justices in Washington did not buy this argument, they unanimously held that companies could be sued for inducing copyright infringements for acts taken in the course of marketing file sharing software. A more distributed and decentralized generation of P2P systems followed as a result of the legal arguments of the Court. The "servent" (server/client) architecture of these networks was adapted to meet the legal constraints of copyright [1, 6]. All in all, we reckon that something similar will occur in the EU law with most of today's blockchain architectures in the field of privacy and data protection.

Next, Section 2 illustrates which specific features of blockchain technologies and hence, what current blockchain networks are under scrutiny in this paper, e.g. closed or open blockchains, rather than, say, Turing-complete or incomplete blockchains. Since some of the data stored in these blockchains are personal, Section 3 takes into account current EU regulation on data protection, i.e. the "GDPR," and more particularly Article 17 on the right to erasure. Certain provisions of Art. 17 appear simply at odds with some properties of blockchains, such as their "immutability." Section 4 considers some solutions for either abiding by the rules of the GDPR, or preventing blockchains from processing personal data. Each solution, so far, has its own drawbacks, as shown by methods of "hashing-out," of keys destruction, of chameleon hash functions, and more. This leads to a paradox. Should we admit that no one-size-fits-all solution exists in this context, except from banning the technology [7]? Should Western countries, e.g. the EU under the GDPR, follow Chinese suit, and throw out the baby (blockchain) with the dirty water (e.g. data illegally stored that have to be erased)?

The conclusion of the paper brings us back to the parallel between the legal fate of P2P systems and current debate on blockchains. As illustrated by the former's cases in the early 2000s, an outright ban of blockchain systems that do not provide mechanisms for erasing data illegally stored is for real. In the jargon of the US Supreme Court, we shall distinguish between technologies capable, or "incapable of non-infringing uses." The paper examines feasible technical solutions, much as the role that social norms and the forces of the market may play in this context. The forecast is twofold: on the one hand, it is likely that the "Grokster mechanism" will reappear in the EU under the GDPR. There will be a new generation of blockchain networks, whose design and architecture intend to abide by the EU provisions on data protection. Yet, on the other hand, we should consider that some current blockchains, such as Bitcoin, operate in

more than 100 different jurisdictions with lack of formal governance, thus suggesting further problems of enforcement. The final outcome of this interplay between law and technology is of course far from clear and, nevertheless, the clash between legal and technological regulations, economic interests, or social values, e.g. trust, seems inevitable. In homage to Gabriel García Márquez 1981 novel, let us start our "chronicle of a clash foretold."

2. Blockchains

There are many definitions of blockchain out there. Some present blockchains as P2P, append-only, tamper-proof, ever-growing distributed and decentralized networks that function as records for transactions [2]. Others insist on the properties of the network that allow the nodes to agree on the order, validity, existence, and authenticity of all the transactions ever occurred within the system [8]. In a nutshell, blockchains link chunks of data together in blocks by including the hash of the previous block, i.e. the function used to map data of arbitrary size to data of a fixed size. By defining the height of a block as the number of blocks in the chain between it and the genesis block, whose height is 0, it follows that a block with height *x* includes the hash of the block with height *x-1*, the block with height *x-1* includes the hash of the block with height *x-2* and so on. This is crucial. Any modification to the data stored in a block necessarily entails having to re-compute all the blocks that came after it, otherwise the system rejects the modified block. We return to this issue later in the next section, where the provisions of the GDPR's right to erasure are illustrated with their pros and cons.

Still, there are different kinds of blockchains, e.g. Turing-complete, or incomplete systems [4]. In this context, dealing with Art. 17 of the GDPR, the distinction between open and closed blockchains is particularly relevant. Open blockchains, such as Bitcoin and Ethereum, are "permissionless"; closed blockchains, such as Corda and Hyperledger Fabric, are vice versa "permissioned," i.e. participants in the system are known. Contrary to politically decentralized blockchains, in which nobody controls the network, permissioned blockchains are "politically centralized" [9]. Therefore, notions of "data processors" and "data controllers" do not seem particularly problematic [7, 10]. They regard at least the validators of the network in light of Articles 24 and 28 of the GDPR.

Things appear legally more complex in the case of some open blockchains. Their design aims to make impossible to tamper the information, namely, once the information is appended on a blockchain according to the protocol rules, it is impossible to alter it without compromising the entire network. In addition, such information should persist through time, because the blockchain has to record all the history of the previous states of the system without ever deleting any part of it. Some argue that blockchains are not immutable but rather, hard to change from the users' side [11]. The aforementioned DAO case, or the Ethereum improvement proposal n. 999, shed light on why some blockchains are better understood as immutable for users and non-users of the technology, while simply hard-to-change for the gatekeepers of the system. Therefore, as occurs with validators of closed blockchains, notions of "data processors" and "data controllers" do not appear particularly complex in this second scenario [7, 10]. Responsibilities related to such notions regard at least the gatekeepers of the network.

But, how about "politically decentralized" blockchains [9]? Should we represent all the nodes in the network as data processors, or even data controllers [7, 10]?

Data processed by blockchains concern two different kinds: system-dependent data and arbitrary data. The former is necessary for the functioning of the system: public network addresses, cryptographic primitives, input and outputs of transactions, or private keys, are examples of system-dependent data. On the other hand, most open blockchains allow users to store arbitrary data, namely, any kind of data. Whilst some system-dependent data might be considered personal data under the GDPR [11], others have found that Bitcoin's blockchain already stores more than 1600 arbitrary files [12], some of which likely contain personal data. There are in addition several methods that allow users to store arbitrary data on Bitcoin's blockchain [13]. Correspondingly, we may suspect that sooner, rather than later, matters of data protection will concern the current functioning of such blockchain networks. Next section explores what kind of obligations data protection and data controllers have in the case of the right to erasure, and how the enforcement of this right may work with different kinds of blockchain in the EU legal system.

3. GDPR's Art. 17

The provisions of Art. 17 are divided into three sections, which correspond to (i) the substantial grounds of the right; (ii) its mechanisms; and, (iii) restrictions, rather than exceptions, of the right to erasure. As to the grounds of the right, data subjects can exercise it—i.e. to obtain from the data controller the erasure of their personal data without undue delay—under six circumstances. According to Art.17(1), they regard (a) cases in which such data are no longer necessary in relation to the purposes for which they were collected, or otherwise processed; (b) withdrawal of consent pursuant to Art. 6(1)(a) and Art. 9(2)(a); (c) objection to the processing pursuant to Art. 21(1); (d) unlawful processing; (e) legal obligations to which the controller is subject; and, (f) personal data that have been collected by information society-services when the data subject was a 'child.'

As to the mechanism set up by Art. 17(2), the data controller has not only to erasure the data. It "shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy and replication of, those personal data." This duty of information by the first data controller shall be related to the "available technology" and "cost of implementation."

As to the limits of the right, Art. 17(3) establishes five cases in which the right to erasure does not apply. They concern (a) the right of freedom of expression and information; (b) compliance with certain legal obligations, to which the controller is subject, e.g. the performance of a task carried out in the public interest; (c) reasons of public interests pursuant to Art. 9(2) and (3); (d) archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes; and, (e) the establishment, exercise or defense of legal claims.

Regardless of the technology or online services under scrutiny, e.g. search engines' liability, the critical parts of this new set of provisions can be summed up in accordance with three issues. First, it is up to the data controller to strike a balance between the request of the data subject—pursuant to Art. 17(1)—and the restrictions set up by Art. 17(3). This means the data controller has to evaluate whether the protection of further

rights and interests, such as freedom of speech, should prevail in a certain case. The mechanism, at work in the field of data protection in Europe since the 2014 ruling of the EU Court of Justice ('EUCoJ') on the right to be forgotten, is not new. The EU version of the 'notice-and-takedown' procedure is well known for example in the field of intellectual property and liability of online service providers [14]. In both cases, it is still an open issue whether this mechanism of 'notice-and-takedown' is consistent with due process provisions in Europe, e.g. ECHR's Article 6 on the 'equality of arms,' which is mentioned by art. 6(2) of the EU Treaty as a source of fundamental rights in the European Union [15]. Although data subjects can always challenge the decisions of data controllers before their national authorities and courts, it remains controversial whether this two step-procedure can guarantee both rights of data subjects and the public interest. For example, after the ruling of the EUCoJ, Google has rejected so far about 56% of delisting requests. Out of this considerable amount of rejected requests, only a negligible percentage appealed to a National Authority, with very few requests to a national Court. In the case of the right to be forgotten, it may be argued, "the European Union has not only ordered Google to comply with European law; it has essentially handed off enforcement of the right in the first instance to Google" [16]. Could such scenario ever apply to the data controllers of some blockchain networks?

The second problem concerns the duty to inform pursuant to Art. 17(2). The latter can be understood either as a toothless mechanism or as a powerful means to safeguard the data subjects. The wording of the regulation on "reasonable steps," "available technology," or "cost of implementation," allows either to be true. At their best possible light, these rather vague provisions may represent a wise mechanism of legal flexibility with which to address the challenges posed by the astonishing advancements in technology and prevent over-frequent revisions to tackle such progress [17]. Yet, it is hard to envisage how the entire chain of controllers of Art. 17(2)—triggered by the request of the data subject pursuant to Art. 17(1)—will end up erasing "any links to, or copy and replication of, those personal data." By taking into account the extra-territorial effects of permissionless blockchains operating in multiple jurisdictions, how shall the EU legislators attain their purpose?

The third set of problems regards the restrictions provided by Art. 17(3)(d) on archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. These provisions make of course sense. Still, pursuant to Art. 89(2) and (3), safeguards and conditions for the processing of personal data are delegated in such cases back to national legal systems, e.g. the divergent provisions of Art. 35 of the German Law and Art. 16 of the Luxembourg Law implementing the norms of the GDPR on "erasure." This delegation of power may either entail a European form of experimental federalism, or trigger threats and risks of fragmentation [17]. For instance, according to certain scholars, this mechanism "will certainly reduce the impact of the regulation as a harmonizing force of data protection regulation in Europe in the context of Big Data, and it will make life harder for companies and organizations operating not just in one but multiple Member States in Europe" [18]. Articles 60, 61, 75(4) and 97(2)(b) of the GDPR provide a number of ways to cope with the centrifugal forces of the system, i.e. methods of coordination between multiple jurisdictions of national supervisory authorities. Still, it seems fair to concede that the first data controller triggered by the data subject's request pursuant to Art. 17(1), may have a hard time in striking a fair balance between this request and the restrictions that shall be often evaluated on a national basis, in accordance with Art. 17(3)(d).

Scholars have extensively discussed the impact of the GDPR on the functioning and design of blockchains [7, 10, etc.]. The specificity of the technology suggests three possible scenarios. First, we can imagine a bunch of GDPR abiding blockchain systems that lawfully process and store personal data: think again about the validators of a permissioned blockchain network, or the gatekeepers of some open blockchains. There is no reason why such networks cannot legally process personal data in accordance with obligations of data processors and data controllers established by the GDPR. Moreover, this compliance represents the bread and butter of several EU projects, e.g. DECODE, in which the aim of lawyers, developers, and other experts, is to design win-win solutions for blockchain-driven projects that process personal data [19].

Yet, something can go wrong. Consider a Court's order to delete personal data on a blockchain pursuant to either Art. 17(1)(d) of the GDPR on unlawful processing, or Art. 17(1)(b) on withdrawal of consent, in accordance with Art. 6(1)(a), or Art. 9(2)(a). Once a Court identifies the data processors and controllers of the blockchain with, say, the gatekeepers of the network, what should the next legal step be? Since irreversibly encrypting personal data on blockchains seems unfeasible [20], should the law force the entire blockchain network to re-compute all the blocks that follow the block in which the network stored the personal data to be erased? But, how about the transactions that occurred after the target block? Are they not at risk? Shouldn't the network halt, until all the subsequent blocks are mined? In more general terms, how should we address the retroactive effect of such measures?

The third scenario is even more worrying. Here, personal data have to be removed from a blockchain pursuant to Art. 17 of the GDPR, and still it is hard to find out who should remove such data; who is, in other words, responsible. After all, one of the mantras in today's debate on blockchains conceives them as a sort of "distributed autonomous organizations" [4]. The intricacy of the interaction between humans and computers can make it extremely difficult to ascertain what is, or should be, the information content of the natural or artificial entity, as foundational to determining the responsibility of individuals. Such cases of distributed responsibility that hinge on multiple accumulated actions of humans and computers may lead to cases of impunity that already have recommended some legal systems to adopt new forms of criminal accountability [21]. In the case of highly distributed networks, such as DAOs, what should the response of the law thus be? After the legal misadventures of P2P systems in the 2000s, will history repeat itself with the ban of some kinds of blockchain networks, e.g. illegal non-modifiable blocks of data and information?

Next section further explores these scenarios with some technical solutions.

4. The Clash

The troubles of blockchains with the GDPR can be examined with some solutions that experts and scholars have proposed over the past years. Most efforts comprehensibly revolve around how to make personal data anonymous on the blockchain. Methods for generating a new public key pair for each transaction have been developed for Bitcoin and Ethereum, whilst cryptographic techniques, such as "ring confidential transactions" [22], and zero-knowledge proofs [23], have been implemented into the Monero and the Z-Cash cryptocurrencies, respectively.

In the case of the right to erasure of personal data, three main approaches have emerged. The first is "hashing-out," that is, storing personal data off-chain in a database

under the control of an identifiable data controller. The blockchain maintains a hash that can be used as a link to the database in which personal data are stored. Once the right to erasure of Art. 17 is triggered, that which should be erased is only the off-chain data that are employed to identify any subject linked to the in-chain hash. The price to pay for this solution, however, seems too high to many: "this [solution] may be considered a betrayal to the decentralization principle of blockchains, as a certain degree of control of data remains in the hands of a single centralized party" [10]. Here, the clash appears as a matter of principle that involves both the design of technology, its architecture, and the distribution of power among the nodes of the network.

The second approach concerns "key destruction." The use of sufficiently strong encryption for data stored on blockchains suggests that data can be "erased" by destroying the encryption key. The information is no longer accessible because it is impossible to decrypt the data. Yet, it is an open question whether the provisions of Art. 17 can be interpreted in such a way, that data should not be really erased from the chain but only accessible by the data subject, or not accessible at all. According to the 2014 Opinion of the Art. 29 Working Party, "state-of-the-art encryption... does not necessarily result in anonymisation" [20]. Correspondingly, the destruction of data or keys does not eliminate the possibility to re-identify individuals. Furthermore, in the Opinion of the EU authorities, hypotheses of brute force attacks and the evolution of technology have also to be taken into account. The clash appears here more as a matter of security standards, than a matter of principle.

The third approach has to do with chameleon hashes. Rather than hashing-out data, or making such data inaccessible with the destruction of the keys, the aim is to devise "redactable blockchains" through the use of hash functions that involve a trapdoor [24]. The knowledge of such trapdoor allows re-writing the blocks under specific constraints, e.g. transparency and accountability. The redaction occurs either through a trusted third party that knows the trapdoor to open the block, or by adding the hash function as a primitive of the blockchain's protocol. In the first case, some of the critiques to the hashing-out approach, i.e. "betrayal to the political decentralization principle," reappear. In the second case, we may wonder how to properly address the data protection issues of most blockchains, since blockchains need to include chameleon hash functions from their own inception in order to be redactable [10]. Moreover, according to some others, "chameleon hashes can't eliminate old copes of the blockchain that will still contain the redacted information and miners also have the discretion as to whether to accept the changes or not" [7, 24]. Here, the reasons for a legal clash appear as a mix of principles on political decentralization and rules for data protection.

Further approaches do exist, e.g. μchains [25]. However, it seems fair to admit that all the solutions illustrated in this section have some problems of their own and, all in all, they appear unfit to deal with the erasure of personal data *already present* in some blockchains today. By further considering multiple types of blockchain, according to their architecture, uses, services, or functions, it is then hard to say what solution to the right to erasure-problem could prevail in the next future. In any event, we should not overlook another reason of clash between today's legal frameworks and most current blockchains. Going back to the final scenario of the previous section on highly distributed networks, such as DAOs—in which it can be tricky to determine who is the data processor, and who is the data controller—the clash concerns regulatory systems that compete and even render the claim of the other regulatory system superfluous.

From the viewpoint of technology as a regulatory system [26], several examples illustrate how the legal intent to regulate the process of technological innovation may

fail. The EU e-money directive 46 from 2000 is instructive: soon after its implementation, further forms of online payments, such as PayPal, forced the Bruxelles legislators to intervene, finally amending themselves with the new directive 110 from 2009. From the viewpoint of the law, however, several counter-examples stress the multiple ways in which legal systems may affect—and even hinder—technological innovation. As shown by the aforementioned 2005 ruling of the US Supreme Court in the Grokster case, the legal parable of P2P systems is instructive. It draws our attention to (i) whether or not a technology should be banned; (ii) whether designers and producers of such technology are accountable; and, (iii) whether users of P2P, and now blockchains, can be held liable as well. In the case of users of highly distributed blockchain networks with no obvious data controller, some argue, "a large amount of nodes would need to be contacted and compelled to comply... this may lead to forcing all nodes to stop running the blockchain software where GDPR rights cannot be achieved through alternative means" [7].

Others claim that even in the case of individuals directly interacting with a permissionless blockchain, a solution can be found through voluntary clauses embedded into the system via smart rules [19], or conditions and terms of use [10]. These latter approaches could indeed strengthen GDPR requirements for lawful data processing, by either prohibiting the processing of certain types of personal data, or requiring users to have consent or another legal basis for processing. According to Art. 25 of the GDPR on the so-called principle of privacy by default and by design, designers and developers of such blockchains could also be forced to embed some of the techniques mentioned in this section, e.g. zero-knowledge proofs, into the design of the blockchain. The problem with this line of argument, however, is that issues are not always 'technical,' but 'social.' Social issues may concern matters of principle on the design of the network and its degrees of 'political decentralization' [9]; namely, the distribution of power among the nodes of a blockchain. In addition, social clash may regard the extra-territorial effects of such distributed blockchain networks [26], their terms of use and enforcement [6], or the consensus algorithm on whose proof-of-work the process of block computing relies in most blockchains [4]. In light of P2P legal misadventures, we may thus expect in the short term either courts potentially targeting the whole bunch of users interacting with a permissionless blockchain, or blocking some blockchains with court orders. This is what already occurred with the Peppermint case on P2P systems in Italy, back to 2008 [27]. Will history repeat itself?

5. Conclusions

One of our main contentions in the paper has been that GDPR abiding blockchain systems are feasible. Jurists, programmers, and other experts are increasingly working on this nowadays. Some argue that blockchain solutions could even strengthen rights and obligations enshrined in the GDPR [7, 10, 19]. Still, manifold blockchain networks functioning out there suggest a new generation of data protection issues brought about by this technology. Some of these issues will likely concern the right to erasure set up by Art. 17. These cases will soon be discussed before national authorities and courts, and will likely test all the solutions that have been illustrated in the previous sections. In the case of permissioned, or closed blockchains, it is arguable that "hashing-out" strategies can properly address Art. 17 related issues. The "betrayal" of the decentralization principle seems however the price to be paid for such solution [9, 10].

In the case of permissionless blockchains, the legal test under the GDPR will often be about "key destruction" techniques, chameleon hashes, or μchains. Yet, we may suspect that some highly distributed blockchain networks will find a harder time with the implementation of Art. 17. Contrary to the legal misadventures of P2P systems, e.g. the 2008 Peppermint case in Italy [27], we think it is unlikely that national authorities and courts will target the bunch of individuals directly interacting with a permissionless blockchain, so as to enforce a data subject's right to erasure. Rather, it is probable that the target will be the blockchain network as such. This was the legal output of another famous P2P case, i.e. the 2005 Grokster case of the US Supreme Court, and this has also been the recent EU policy on other crucial issues of internet governance, such as liability of search engine services as controllers of personal data processing. It is thus likely that this trend will go on with some blockchain cases, "forcing all nodes to stop running the blockchain software" [7].

The parallel with the legal issues of P2P systems sheds light on two further aspects of today's debate on legal blockchains. First, in the phrasing of the US Supreme Court, there is no doubt that blockchain networks are "capable of non-infringing uses." Contrary to many 2000s, early 2010s opponents of P2P systems, there is no Western advocate of the ban of blockchain technologies up today. This is not to say that current blockchains are business as usual in the legal domain, and should not be rather re-conceptualized, and accordingly designed. The paper illustrated some solutions, e.g. chameleon hash functions and zero-knowledge proofs, which should be embedded into the design of the blockchain since its inception, in order to prevent data protection-related issues. The reference point of the GDPR was here Article 25 on privacy by design, and by default. This brings us to the second facet of our parallel. In the case of P2P networks, the 2005 decision of the US Supreme Court represented a threshold for the design of these systems: after the ruling of Justices in Washington, the design solution for the most relevant legal issue of many P2P systems, e.g. copyright infringement, was a more decentralized and distributed architecture for such file-sharing networks [1]. In the case of blockchains, it is likely that we will similarly refer soon to their architecture, by distinguishing between blockchains designed before or after the GDPR. The threshold indicates the set of blockchains that have been thought about to expressly meet the requirements of the EU regulation through e.g. privacy by design techniques, and blockchains that, for one reason or another, e.g. ante GDPR designed blockchains, trigger some sort of clash with the legal order. The paper has sorted out four different kinds of clash, i.e. on principles, security standards, rules for data protection, and 'social clashes.' It is unclear how the interplay between legal regulation, technological constraints, social norms, and market interests, will end up in this context; still, we should be ready to address, or even prevent, such different kinds of clashes. Rulings and court orders will be instructive over the next years.

References

[1] A. Glorioso, G. Ruffo, and U. Pagallo, The Social Impact of P2P Systems, in X. Shen, H. Yu, J. Buford and M. Akon, *Handbook of Peer-to-Peer Networking*, pp. 47-70, Springer Heidelberg, 2010.

[2] R. Wattenhofer, *The science of the blockchain*, CreateSpace Independent Publishing Platform, 2016.

[3] M. Bauwens, *P2P and Human Evolution: Placing Peer to Peer Theory in an Integral Framework*, at http://integralvisioning.org/article.php?story=p2ptheory1, 2005 (last accessed April 20th, 2018).

[4] M. Crepaldi, The path toward an ethics of Distributed Autonomous Organizations (DAOs), *Ethicomp* Proceedings, September 2018.

[5] M. Campbell-Verduyn (ed.), *Bitcoin and Beyond Cryptocurrencies, Blockchains, and Global Governance*, Routledge New York, 2018.
[6] U. Pagallo and M. Durante, Three roads to P2P systems and their impact on business ethics, *Journal of Business Ethics* **90** (2009), 551-564.
[7] M. Finck, Blockchain and Data Protection in the European Union. *Max Planck Institute for Innovation & Competition, Research Paper No. 18-01*, 2017 (Available at SSRN https://ssrn.com/abstract=3080322 or http://dx.doi.org/10.2139/ssrn.3080322).
[8] F. Glaser, Pervasive decentralization of digital infrastructures: a framework for blockchain enabled system and use case analysis, 2017.
[9] V. Buterin, The Meaning of Decentralization, available at https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274, February 2017.
[10] L-D. Ibáñez, K. O'Hara and E. Simperi, On Blockchains and the General Data Protection Regulation, University of Southampton, June 2018.
[11] A. Walch, A. The path of the blockchain lexicon (and the law), 2017.
[12] R. Matzutt, J. Hiller, M. Henze, J.H. Ziegeldorf, D. Müllmann, O. Hohlfeld, and K. Wehrle, *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin.* Paper presented at the Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer, 2018.
[13] A. Sward, I. Vecna, and F. Stonedahl, F., Data Insertion in Bitcoin's Blockchain. *2018, 3*. doi:10.5195/ledger.2018.10,1
[14] P. Van Eecke, Online service providers and liability: A plea for a balanced approach, *Common Market Law Review* **48**(5) (2011), 1455–1502.
[15] U. Pagallo and M. Durante, Legal Memories and the Right to Be Forgotten, in L. Floridi (ed.), *Protection of Information and the Right to Privacy. A New Equilibrium?,* Law, Governance and Technology Series 17, Springer, Dordrecht, 2014, 17-30.
[16] J.M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation (September 9, 2017). *Yale Law School, Public Law Research Paper No. 615*. Available at SSRN: https://ssrn.com/abstract=3038939.
[17] U. Pagallo, The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection **3**, 1 (2017), 34-46.
[18] V. M. Schönberger and Y. Padova, Regime change? Enabling big data through Europe's new data protection regulation, *Columbia Science and Technology Law Review* **17** (2016), 315-335.
[19] E. Bassi, M. Ciurcina, J.C. De Martin, S. Fenoglietto, G. Rocchi, O. Sagarra Pascua, and F. Bria, D1.8 Legal Framework for Digital commons DECODE OS Legal Guidelines, Decode Project, 2017., available at https://www.decodeproject.eu/publications/legal-frameworks-digital-commons-decode-os-and-legal-guidelines.
[20] Art. 29 Working Party, Opinion on Anonymization Techniques, n. 05/2014.
[21] U. Pagallo, AI and Bad Robots: The Criminology of Automation, in M.R. McGuire and Th. J. Holt (eds.), *The Routledge Handbook of Technology, Crime and Justice*, 643-653. London & New York, Routledge, 2017.
[22] S. Noether, A. Mackenzie, and the Monero Research Lab, Ring Confidential Transactions, *Ledger* **1**(1), December 2016.
[23] E. Ben-Sasson, A. Chiesa, E. Tromer and M. Virza, Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. Technical Report 879, 2013.
[24] G. Ateniese, B. Magri, D. Venturi, E. Andrade, Redactable Blockchain–or–rewriting History in Bitcoin and Friends*. Security and Privacy (EuroS&P)*, IEEE European Symposium, 2017.
[25] I. Puddu, A. Dmitrienko, S. Capkun,. µchain: How to Forget without Hard Forks. *IACR Cryptology ePrint Archive*, December 2017.
[26] U. Pagallo, The Realignment of the Sources of the Law and their Meaning in an Information Society, Philosophy & Technology **28**, 1 (2015), 57-73.
[27] U. Pagallo, Let Them Be Peers: The Future of P2P Systems and Their Impact on Contemporary Legal Networks, in M. Fernandez-Barrera, N. Nuno Gomes de Andrade, P. de Filippi, M. Viola de Azevedo Cunha, G. Sartor e P. Casanovas (eds.), *Law and Technology: Looking into the Future*, pp. 323-338. European Press Academic Publishing, Florence, 2009.