

# *How to Make Sure My Cryptokitties Are Here Forever? The Complementary Roles of Blockchain and the Law to Bring Trust*

Charlotte DUCUING\* 

---

*Under the phrase “code is law” and based on its “trustless trust”, blockchain has emerged as a disrupting technology considered by some as an alternative to the law. Based on a study of real-life blockchain-based decentralised applications (Dapps), this article takes blockchain developers at their word and adopts the point of view of users: can blockchain live up to its promise and enable them to transact with each other without the need for the trust granted by the law? The article particularly highlights that users need to be able to ascertain that a self-advertised Dapp indeed qualifies as one. Blockchain technology may make it possible to do away with trust in third parties, but this is not enough. Users also need to trust that an alleged Dapp genuinely is one, and blockchain alone cannot provide this. Beyond Dapps, it is argued that blockchain needs the complementary role of the law to deliver its promises and especially to authenticate blockchain “virtues”. The EU certification mark is identified as a promising form of co-regulation for that purpose.*

## I. INTRODUCTION: BLOCKCHAIN-BASED DECENTRALISED GOVERNANCE AND THE PROMISE OF TRUSTLESS TRUST

The first wave of blockchain technology was characterised by the rise of cryptocurrencies – the first of them being Bitcoin – which enabled decentralised electronic payment while circumventing financial institutions. But the potential of blockchain technology is not limited to currencies. As highlighted by Davidson et al, “distributed ledgers are a technology of decentralization”.<sup>1</sup> Blockchain would make it possible to perform activities without the intermediaries traditionally needed to bring trust between parties<sup>2</sup>, by replacing them with “the network of participants”<sup>3</sup> based on computationally-achieved

---

\* [charlotte.ducuing@kuleuven.be](mailto:charlotte.ducuing@kuleuven.be).

<sup>1</sup> S Davidson et al, “Blockchains and the Economic Institutions of Capitalism” (2018) 14(12) *Journal of Institutional Economics* 639.

<sup>2</sup> A Wright and P De Filippi, “Decentralized Blockchain Technology and the Rise of Lex Cryptographia” (Social Science Research Network 2015) SSRN Scholarly Paper ID 2580664 2.

<sup>3</sup> S DiRose and M Mansouri, “Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations”, 2018 13th Annual Conference on System of Systems Engineering (SoSE) (2018).

consensus. Actors could “trust the technology, which dispenses from the need to trust human counterparties or institutions”.<sup>4</sup> This feature – also known as trustless trust<sup>5</sup> or “trust-by-computation”<sup>6</sup> – is the overarching purpose of blockchain. In that sense, blockchain technology has been described as an “institutional technology”.<sup>7</sup> Other blockchain protocols have been further developed to decentralise various activities, such as information storage and sharing,<sup>8</sup> registries,<sup>9</sup> domain name systems,<sup>10</sup> transfer of assets (“smart property”),<sup>11</sup> capital markets,<sup>12</sup> voting systems,<sup>13</sup> enforcement of contracts without the need to resort to judiciary authorities (“smart contracts”),<sup>14</sup> and the list keeps growing.

Against this background, the decentralisation of *governance* by means of blockchain-based automation is considered as the “final stage of decentralization”<sup>15</sup> and attracts much attention. Coordination between individuals to make decisions is a difficult task that requires organisational models. Until the blockchain technology emerged, it had been mainly achieved by trusting a third party to do so (agency model). Detrimental effects are observed when this party becomes an inevitable intermediary, such as abuse of such central position<sup>16</sup> or high costs. More generally this party constitutes a “single point of failure” (in blockchain parlance), thereby concentrating the risks. The party can be a public authority, such as elected politicians governing a State or appointed institutions such as central banks. It can also be a private entity, such as the GAFAM or Uber, accused of taking advantage of their respective gatekeeping positions to exploit the value brought by the users. The idea is that blockchain provides for “governance-by-computation”<sup>17</sup> or “trustless trust”, enabling individuals to reach consensus and make common decisions in a distributed manner, without having to delegate this competence to trusted third parties.<sup>18</sup> Among other things, the

<sup>4</sup> M Finck, “Blockchains: Regulating the Unknown” (2018) 19(4) German Law Journal 665.

<sup>5</sup> This broadly used expression is credited to have been coined by Reid Hoffman, see R Hoffman, “The Future of the Bitcoin Ecosystem and ‘Trustless Trust’ – Why I Invested in Blockstream”, *LinkedIn* post, 17 November 2014, <[www.linkedin.com/pulse/20141117154558-1213-the-future-of-the-bitcoin-ecosystem-and-trustless-trust-why-i-invested-in-blockstream/](http://www.linkedin.com/pulse/20141117154558-1213-the-future-of-the-bitcoin-ecosystem-and-trustless-trust-why-i-invested-in-blockstream/)> (last accessed 4 July 2019).

<sup>6</sup> M Atzori, “Blockchain Technology and Decentralized Governance: Is the State Still Necessary?” (2017) 6 Journal of Governance and Regulation 45 at p 46.

<sup>7</sup> Davidson et al, *supra*, note 1, p 646.

<sup>8</sup> P De Filippi and A Wright, *Blockchain and the Law* (Harvard University Press 2018) Ch 1 “Blockchains, Bitcoin, and Decentralized Computing Platforms” p 29.

<sup>9</sup> Wright and De Filippi, *supra*, note 2, p 28.

<sup>10</sup> *ibid*, p 14.

<sup>11</sup> *ibid*, pp 33–36.

<sup>12</sup> De Filippi and Wright, *supra*, note 8, p 98.

<sup>13</sup> Atzori, *supra*, note 6, p 47.

<sup>14</sup> Wright and De Filippi, *supra*, note 2, p 10.

<sup>15</sup> Atzori, *supra*, note 6, p 51.

<sup>16</sup> K Werbach, “Trust, but Verify: Why the Blockchain Needs the Law” (2018) 33 Berkeley Technology Law Journal 487 at p 509–510.

<sup>17</sup> Atzori, *supra*, note 6, p 54.

<sup>18</sup> P Ortolani, “The Three Challenges of Stateless Justice” (2016) 7 Journal of International Dispute Settlement 596; M Jun, “Blockchain Government – a next Form of Infrastructure for the Twenty-First Century” (2018) 4 Journal of Open Innovation: Technology, Market, and Complexity 7. The author considers that the blockchain would constitute “absolute law”. P De Filippi and S Hassan, “Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code” (2016) 21 First Monday; WA Kaal and C Calcaterra, “Crypto Transaction Dispute Resolution” (2017) 73 The Business Lawyer 109 at p 144. The authors consider that “blockchain technology provides its own solutions for jurisdictional issues, governance and conflict resolution”.

possibility for blockchain technology to “transform the gig economy”<sup>19</sup> and get rid of digital platforms intermediaries has been put forward. Blockchain is also envisaged as a means to organise (digital) commons.<sup>20</sup>

The blockchain community has then abounded in technical writings to try and achieve blockchain-based decentralised services and organisations. The latter may consist of stand-alone blockchain networks, or they can “run” on another blockchain network, such as Ethereum. Ethereum was indeed created as a non-specific network-powered super-computer<sup>21</sup> on which programmers can run any application<sup>22</sup> so that it functions as a disinterested intermediary enabling other e-commerce services to take place on the application layer. In his ambition to create a fully decentralised e-commerce ecosystem as an alternative to the current one, which he deemed too centralised, V Buterin, the founder of Ethereum V, especially envisioned “decentralised applications” (Dapp, ÐApp or DA) to run on the Ethereum network<sup>23</sup> “instead of running on a central server as usual Apps”<sup>24</sup> amongst which he singled out “Decentralized (Autonomous) Organizations” (DAOs).<sup>25</sup> The list of decentralised (autonomous) entities has then extensively grown in the blockchain community and in the scholarship with reference to corporations, societies (respectively D(A)Cs and D(A)Ss),<sup>26</sup> government (DAG),<sup>27</sup> Decentralised Collaborative Organization (DCO)<sup>28</sup> or delegated Decentralized Autonomous Organization (dDAO)<sup>29</sup> according to the entity to be “decentralised” as well as to its actual means and purpose.

DAOs are being largely discussed within the blockchain community and in the scholarship as the most ambitious form of blockchain-based decentralised entity.<sup>30</sup> According to Buterin who coined the term, a DAO “is an entity that lives on the internet and exists autonomously [ . . . ]”. The autonomy of a DAO means that it “in some fashion, makes decisions for itself”. For example, Buterin considers the Bitcoin network to be autonomous enough to qualify as a DAO, rather than as a mere decentralised organization (DO). One feature common to

---

<sup>19</sup> J Pouwelse et al, “Laws for Creating Trust in the Blockchain Age” (2017) 6 European Property Law Journal 321 at p 323.

<sup>20</sup> Davidson et al, *supra*, note 1, p 654; V Papadimitropoulos, “Reflections on the Contradictions of the Commons” (2018) 50(2) *Review of Radical Political Economics* 317.

<sup>21</sup> The Ethereum white paper refers to the Ethereum blockchain as a “virtual machine”: Buterin et al, “A Next-Generation Smart Contract and Decentralized Application Platform (‘Ethereum White Paper’)” <[github.com/ethereum/wiki/wiki/White-Paper](https://github.com/ethereum/wiki/wiki/White-Paper)> (last accessed 4 July 2019).

<sup>22</sup> V Shermin, “Disrupting Governance with Blockchains and Smart Contracts” (2017) 26 *Strategic Change* 499.

<sup>23</sup> Buterin et al, *supra*, note 21.

<sup>24</sup> B Arruñada and L Garicano, “Blockchain: The Birth of Decentralized Governance” *Pompeu Fabra University, Economics and Business Working Paper Series 1608*, p 6.

<sup>25</sup> “DAO” was also used to refer to “Distributed Autonomous Organization” (emphasis added), in Davidson et al, *supra*, note 1, p 5; and Finck, *supra*, note 4, p 7.

<sup>26</sup> Atzori, *supra*, note 6, p 46.

<sup>27</sup> Jun, *supra*, note 18.

<sup>28</sup> Davidson et al, *supra*, note 1, p 7.

<sup>29</sup> DiRose and Mansouri, *supra*, note 3.

<sup>30</sup> Werbach, *supra*, note 16, pp 506–507.

both DO and DAOs is the decentralised character of the organisation, meaning that “instead of a hierarchical structure managed by a set of humans interacting in person [...] a decentralized organization involves a set of humans interacting with each other according to a protocol specified in code, and enforced on the blockchain”. According to Buterin, a DAO is a Dapp with the main additional feature that it “has internal capital”.<sup>31</sup>

As for the Dapp, the most elaborate definition within the blockchain community was proposed by Johnston et al in 2015<sup>32</sup> and has since been massively re-used.<sup>33</sup> According to the authors, an application is genuinely “decentralised” if it meets the four following criteria: (1) it is fully open-source and “operates autonomously” with “no entity controlling the majority of its tokens” while changes to the protocol are “decided by consensus of its users”; (2) the “application’s data and records of operation are cryptographically stored in a public decentralized blockchain in order to avoid any central points of failure”; (3) the application “uses a cryptographic token [...] necessary for access to the application and any contribution of value [...] should be rewarded in the application’s tokens”; and finally (4) it must “generate tokens according to a standard cryptographic algorithm acting as a proof of the value nodes are contributing to the application [...]”. Bitcoin is cited as an example of a Dapp. The definition refers both to technical and governance criteria with the aim to prevent single points of failure and political centralised control of the application. Being a Dapp would ensure the presence of blockchain characteristics in the governance of the application and notably its autonomous character so that no trust in third parties would be needed.<sup>34</sup>

This article takes blockchain developers at their word and adopts the point of view of the users: *Can blockchain live up to its promise and enable them to transact with each other without the need for the trust granted by the law?* The article particularly focuses on the need of users to ascertain and *trust* that a self-advertised Dapp (or other blockchain-based entity) does indeed qualify as one. While blockchain technology may enable the creation of Dapps, section II below, based on real-life examples, shows why users also need to be able to *authenticate* Dapps as being genuinely so. Having found, in section III, that the blockchain environment at large is not able to provide such authentication, section IV then identifies the missing component as, essentially, the legal function of classification of regulatory objects. Finally, some legal options are outlined where certification mark is identified as an interesting form of co-regulation for that purpose.

<sup>31</sup> V Buterin, “DAOs, DACs, DAs and More: An Incomplete Terminology Guide” (6 May 2014), available at <[blog.etherbase.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/](http://blog.etherbase.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/)> (last accessed 11 July 2019).

<sup>32</sup> D Johnston et al, “Decentralized Applications White Paper and Spec. Contribute to DavidJohnstonCEO/DecentralizedApplications Development by Creating an Account on GitHub” (2018) <[github.com/DavidJohnstonCEO/DecentralizedApplications](https://github.com/DavidJohnstonCEO/DecentralizedApplications)> (last accessed 4 July 2019).

<sup>33</sup> This definition is notably referred to in the study of the European Parliament on blockchain technology: P Boucher, “How blockchain technology could change our lives” European Parliamentary Research Service, 2017, 20.

<sup>34</sup> E Mik, “Smart Contracts: Terminology, Technical Limitations and Real World Complexity”, available at <[papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3038406](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038406)>. The author highlights the following belief (a statement that she then criticises): “if the platform itself is trustless, there is no need for any third parties to [...] reduce the transactional risks that are present on an insecure platform. On a trustless platform, such risks are simply absent”.

## II. A NEED FOR META-TRUST...

A fair number of websites operate on the internet and claim to be “Dapps”, DAOs and the like. Among others, Storj<sup>35</sup> operates decentralised cloud storage, LaZooz<sup>36</sup> decentralised carpooling, Cryptokitties<sup>37</sup> provides “digital cats” collectibles, Kleros<sup>38</sup> provides blockchain-based arbitration and OpenBazaar<sup>39</sup> operates a decentralised online marketplace. For instance, Kleros advertises itself as a “decentralized application” and “autonomous application” providing a blockchain-based arbitration service. “Every step of the arbitration process (securing evidence, selecting jurors, etc) is fully automated. Kleros does not rely on the honesty of a few individuals but on game-theoretical economic incentives” [enshrined in the Kleros protocol].<sup>40</sup> Such “computational courts”<sup>41</sup> obviously pose legal challenges arising from their attempt to constitute an alternative to judicial dispute resolution, which are, however, not the subject-matter of this paper: our point here is that blockchain-based decentralisation is a core feature of the service delivered by Kleros. As a result, Kleros users are invited to *trust blockchain protocol* as enabling “crowdsourced jurors to adjudicate disputes”. Failing that, the users would be left with their dispute being arbitrated by anonymous jurors about whom they have no guarantee.

In a different fashion, CryptoKitties, advertises itself as a “distributed application” and a Dapp which provides users with a game consisting of “breeding and collecting” unique digital cats. The advertising states that, “secure in the knowledge that blockchain will track ownership securely”, a digital cat is “100% owned by you; it cannot be replicated, taken away, or destroyed”. The underlying argument is that of the immutability and tamper-proof character of a public and decentralised blockchain, so that the application’s data stored on it (the second condition for being a Dapp), in this case the data featuring the digital cats, are also immutable because they would not depend upon a third party being a “single point of failure”. The characterisation as Dapp hence also plays a role in the essential features of the service provided. These websites look like any other website,<sup>42</sup> only their marketing highlights their blockchain virtues. The use of blockchain terminology – and especially the signs of “Dapp” or DAO recognised in the blockchain community – triggers expectations of decentralisation and absence of single point of failure on behalf of the users. However, such marketing may simply be misleading.

A user of CryptoKitties argued that “CryptoKitties folks”<sup>43</sup> retain the ability to alter, duplicate and even destroy the digital cats. In other words, the application would not be as decentralised and autonomous as promoted. Therein, CryptoKitties Terms of Use

<sup>35</sup> See <[storj.io/](http://storj.io/)> (last accessed 4 July 2019).

<sup>36</sup> See <[lazooz.org/](http://lazooz.org/)> (last accessed 4 July 2019).

<sup>37</sup> See <[www.cryptokitties.co/](http://www.cryptokitties.co/)> (last accessed 4 July 2019).

<sup>38</sup> See <[kleros.io](http://kleros.io/)> (last accessed 4 July 2019).

<sup>39</sup> See <[openbazaar.org](http://openbazaar.org/)> (last accessed 4 July 2019).

<sup>40</sup> Lesaege and Ast, *Kleros Short Paper* v.1.0.5, January 2018.

<sup>41</sup> Werbach, *supra*, note 16, p 545.

<sup>42</sup> Wright and De Filippi, *supra*, note 2, 21.

<sup>43</sup> Zhang, Your CryptoKitty Isn’t Forever – Why DApps Aren’t as Decentralized as You Think, 3 December 2017, <[medium.com/loom-network/your-crypto-kitty-isnt-forever-why-dapps-aren-t-as-decentralized-as-you-think-871d6acfea](https://medium.com/loom-network/your-crypto-kitty-isnt-forever-why-dapps-aren-t-as-decentralized-as-you-think-871d6acfea)> (last accessed 4 July 2019).

stipulate that “in addition to the Gas Fee [the cost of running smart contracts transactions on the underlying Ethereum blockchain], each time you utilize the CryptoKitties marketplace Smart Contract to conduct a transaction with another user via the App, you authorize us [namely Dapper Labs Inc] to collect a commission of 3.75% of the total value of that transaction [ . . . ]”.<sup>44</sup> This tends to confirm that a single legal entity, namely Dapper Labs Inc, would run the application. Except for the Terms of Use referring to a contractual arrangement between the consumer and “Dapper Labs Inc”, the rest of the website, and especially the homepage, is however silent on who is actually running CryptoKitties and refers more profusely and confusedly to “the Cryptokitties team”. Given that CryptoKitties obviously targets individuals, the marketing of CryptoKitties could *inter alia* constitute an unfair commercial practice within the meaning of Unfair Commercial Practices Directive,<sup>45</sup> and more specifically a “misleading action” in that it would contain “false information and [would] therefore [be] untruthful [ . . . ] in relation to the main characteristics of the product [in casu: the digital cats] and which is likely to cause [a consumer] to take a transactional decision that he would not have taken otherwise”.<sup>46</sup> Illegitimately promoting one’s application as vested with the decentralised virtues of a Dapp – as alleged with regard to CryptoKitties – would obviously also result in misleading consumers with regard to the trader’s role and rights in the transaction, which constitutes another “misleading action”.<sup>47</sup> Illegitimate promotion of the decentralised character of the structure could even quite simply mislead users as to the very *existence* of a trader conducting the economic activity.

Users could also simply be led to believe that there is no “trader” in the traditional sense. Even more seriously, the promotion of blockchain magic is likely to blur the issue enough for users, so that they don’t even *wonder about* the existence of a trader. This is all the more so, given that blockchain decentralisation is sometimes precisely advocated as an alternative to the law under the “code is law” motto.<sup>48</sup> The user would then not even consider that (consumer) law might be applicable to his situation, nor against whom he could invoke it. In this regard, ill-founded promotion of blockchain-based decentralisation – and especially alleged Dapps – may be found not only to constitute unfair commercial practices: they may violate the most basic information obligations provided for in the E-Commerce Directive<sup>49</sup> in order to bring trust in e-commerce, such as the obligation falling onto the provider of an information society service to “render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: (a) the name of the service provider; (b) [his] geographic address; [ . . . ]

<sup>44</sup> CryptoKitties Terms of Use, Art 2.C (version last updated 15 November 2018, <[www.cryptokitties.co/terms-of-use](http://www.cryptokitties.co/terms-of-use)>) (last accessed 4 July 2019).

<sup>45</sup> Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L 149/22 (the UCP Directive).

<sup>46</sup> *ibid*, Art 6(1)(b).

<sup>47</sup> *ibid*, Art 6(1)(f).

<sup>48</sup> De Filippi and Hassan, *supra*, note 18. The phrase “code is law” was first used by Lawrence Lessig, *Code* (Version 2.0, Basic Books 2006) p 20.

<sup>49</sup> Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce [2000] OJ L 178/1 (E-Commerce Directive).



(d) [...] the trade register in which [he] is entered and his registration number [where relevant]”. The legal analysis against the Unfair Commercial Practices and the E-Commerce Directives is only provided as a case in point which has the advantage of being harmonised at EU level, while similar conclusions could also be drawn from the analysis of other bodies of legislation, such as the general principles of fairness and fair dealing in contract law as embodied in the respective national legislations.

Our purpose is not to undertake an audit of the websites promoting themselves as blockchain-based decentralised entities. Rather, the imbalance of information between these entities (“operators) on the one hand and their users on the other hand, demonstrably appears to make it possible for abuses to go unnoticed and unchallenged. Blockchain and the marketing on its “magic” act as a screen between (in this case) consumers and the legal protection afforded to them, rendering the whole legal protection inoperable or at the very least inefficient. The same has already been well documented with regard to the sale of “ICOs” to investors unable to ascertain whom they purchase tokens from, and what the tokens actually consist of.<sup>50</sup> By developing the application of blockchain beyond the realm of the financial sector, the second wave of blockchain only makes this very same issue bigger and broader in scope. It disempowers users, who may not even realise the abuse and who would in any case have a hard time claiming their rights, where in theory available. This leads us to an intermediary conclusion: blockchain technology may make it possible to do away with trust in third parties, but this is not enough. It remains to be seen how users can trust that an alleged blockchain-based application or entity is indeed vested with such blockchain characteristics, or – in other words – that it is what it claims to be. The need for trust does not disappear with blockchain; it is shifted to a meta-level: how to trust that a structure is indeed vested with the ‘trustless trust’ features of the blockchain? In other words, how to bring about what we hereby call “meta-trust”? The importance of this requirement should not be underestimated. Failing to address it is likely to result in free riding behaviours. In the medium term, this could result in what is known in economics as “adverse selection”<sup>51</sup> and would additionally have a chilling effect on the acceptance of blockchain innovations.<sup>52</sup> Against this background, the rise of private blockchains can be seen as a first reaction to the need for trust and accountability. The fact that this disintermediation technology is operated by big IT companies, who were precisely the targets of disintermediation, is not as paradoxical as it might first seem.<sup>53</sup> The next section investigates whether the blockchain environment at large might bring meta-trust or, conversely, what are the hurdles to its doing so.

---

<sup>50</sup> Werbach, *supra*, note 16, p 518.

<sup>51</sup> The expression was coined in GA Akerlof, “The Market for ‘Lemons’: Quality Uncertainty and the Market Mechanism” (1970) 84 *The Quarterly Journal of Economics* 488.

<sup>52</sup> The lack of understandability of the blockchain vocabulary as hindrance to broader acceptability is taken as a given in J de Kruijff and H Weigand, “Towards a Blockchain Ontology” (2017).

<sup>53</sup> K Yeung, “Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law” (2019) 82 *The Modern Law Review* 207, 219. She quotes Paech, who argues that “blockchain financial networks are much more likely to take the form of permissioned networks, involving clear control nodes [...]”.

### III. . . . WHICH CANNOT BE PROVIDED BY THE BLOCKCHAIN

The blockchain environment is not a structured one: it is comprised of a multitude of individual initiatives, brought together by common traits and common beliefs. As part of the latter, the importance of the open-source character of blockchain code is put forward as a regulatory means. The open-source character of the code is unanimously considered as a *sine qua non* condition for qualifying as a Dapp (see definition of a Dapp above), a DAO and the like. Blockchain-based decentralised entities are “inspired from the models of open source collaboration”.<sup>54</sup> Among other virtues, the open-source character of the code would enable collaboration of the “community” in the updates and improvements of the code, and also its auditability.<sup>55</sup> In that sense, the open-source character of the code is a transparency or even accountability<sup>56</sup> measure viewed as a safeguard and can thus be interpreted as vested with a regulatory function.<sup>57</sup> As a matter of fact, some websites have emerged which display the result of their “audit” on existing Dapps.<sup>58</sup> However, mere auditability of the underlying code of a Dapp is clearly not sufficient to enable users to trust the blockchain virtues of an alleged Dapp. It has already been found that “such [open source] networks present major cognitive entry barriers”.<sup>59</sup> This is particularly problematic in the case analysed here of non-developer individuals willing to purchase goods or services on Dapps, or in other words where the blockchain technology would scale up. Further, mere auditing of the open-source code may not be sufficient to determine the level and scope of decentralisation of an application or entity as, simply, not everything is in the code. For instance, a party may use different devices and credentials to control an entity which makes it difficult to trace, especially because anonymity – or at least pseudonymity, is strongly promoted in the blockchain environment.

Failing to determine the decentralised character of an application or structure, users may turn to reputed websites that have emerged on the internet<sup>60</sup> and provide directories of decentralised applications and entities, especially of Dapps. Such websites can easily be found; they are broadly referred to not only within the blockchain community but also in the scholarship.<sup>61</sup> They display Dapps according to criteria such as their field of activity, their popularity, their respective volume of transactions, etc. Users of decentralised applications or entities may therefore want to rely on these directories to be able to determine whether a website is genuinely decentralised, or in other words whether it is a genuine Dapp. As they stand, the directories of Dapps that can be found on the internet are, however, not able to provide such trust service, which is now further analysed by taking a closer look at one of most famous ones, State of the DApps. This website claims it has “become

<sup>54</sup> De Filippi and Wright, *supra*, note 8, p 136.

<sup>55</sup> Atzori, *supra*, note 6, p 51.

<sup>56</sup> A Garapon and J Lassègue, *Justice digitale* (PUF, 2018) p 150.

<sup>57</sup> Wright and De Filippi, *supra*, note 2, p 16.

<sup>58</sup> See <[www.dappsfund.com](http://www.dappsfund.com)> (last accessed 4 July 2019).

<sup>59</sup> Atzori, *supra*, note 6, p 57.

<sup>60</sup> See <[www.stateofthedapps.com/](http://www.stateofthedapps.com/)> (last accessed 4 July 2019). It is referred to on multiple blockchain-related websites and forums. See also, among others <[dappradar.com/](http://dappradar.com/)> (last accessed 4 July 2019).

<sup>61</sup> See for instance Werbach, *supra*, note 16, p 506.



one of the biggest reference for the Ethereum ecosystem<sup>62</sup> and advertises its references (talks, workshops, etc). However, it stipulates in its Terms of Use that “neither the website nor any of the persons or entities involved in any way in respect of the website including its host and its contributors, provide for specific legal, fiscal, economical and/or any other kind of advice or recommendation that may be relied upon. A visitor of the website will therefore act at its own risk in accessing or in any way relying on the content of the website [...]”,<sup>63</sup> especially when investing in cryptocurrencies. Further, State of the DApps does not clarify how a website ends up being displayed as a Dapp in its directory. While the State of the DApps does not claim to be a Dapp or another blockchain-based decentralised entity itself, it does not allow the user to identify who runs the website.<sup>64</sup> In addition, it provides for specific features that Dapps representatives may choose to purchase – upon payment – to enhance the visibility of Dapps “to attract more users”.<sup>65</sup> As a result, one is led to believe that the displaying of Dapps is probably done without any verification of the genuine character of an application as a Dapp so that the State of the DApps would merely be a list of self-proclaimed Dapps. In that it allows for promotion of self-proclaimed Dapps, it can even contribute to further misleading the Dapp users. In this regard, CryptoKitties is, for instance, referred to on State of the DApps with much visibility.<sup>66</sup>

The scholarship has documented – especially in the case of cryptocurrency wallet service providers – the fact that, by creating a new and complex economic environment, blockchain networks give rise to profitable “edge services”,<sup>67</sup> ie intermediaries taking advantage of the lack of knowledge of users of blockchain “things”, while not being “decentralised” themselves.<sup>68</sup> State of the DApps is demonstrably one of those. The very existence of such directories can be viewed as a symptom of the need for reliable information and trust on behalf of users of blockchain things, and in particular alleged decentralised applications and entities.

Eventually, the role of blockchain vocabulary in this regard needs to be touched upon, and especially the role of the taxonomy of blockchain-based decentralised “things” that has been developed. The lack of clarity and reliability of blockchain vocabulary has already been documented.<sup>69</sup> It is paradoxically illustrated by the huge number of websites displaying blockchain glossaries, lexicons or dictionaries.<sup>70</sup> The legal

---

<sup>62</sup> See <[www.stateofthedapps.com/about](http://www.stateofthedapps.com/about)> (last accessed 4 July 2019).

<sup>63</sup> Terms of Use of State of the Dapps, Art 1 <[www.stateofthedapps.com/terms](http://www.stateofthedapps.com/terms)> (last accessed 4 July 2019). See also the Terms of Use, Art 5.

<sup>64</sup> The section “about” refers to State of the DApps as a “not-for-profit curated directory of Decentralized Applications”, *supra*, note 62.

<sup>65</sup> See <[www.stateofthedapps.com/promoted-dapps](http://www.stateofthedapps.com/promoted-dapps)> (last accessed 4 July 2019).

<sup>66</sup> It is notably reported in the list of “top Dapps” accessible on <[www.stateofthedapps.com/rankings](http://www.stateofthedapps.com/rankings)> (last accessed 4 July 2019).

<sup>67</sup> Werbach, *supra*, note 16, pp 512–513.

<sup>68</sup> Atzori, *supra*, note 6, p 58.

<sup>69</sup> Mik, *supra*, note 34; A Walch, “Blockchain’s Treacherous Vocabulary: One More Challenge for Regulators” (2017) 21 *Journal of Internet Law* 1 at p 10.

<sup>70</sup> Among many others, see <[www.technologyreview.com/s/610885/a-glossary-of-blockchain-jargon/](http://www.technologyreview.com/s/610885/a-glossary-of-blockchain-jargon/)>, <[blockgeeks.com/guides/blockchain-glossary-from-a-z/](http://blockgeeks.com/guides/blockchain-glossary-from-a-z/)>, and <[blockchainhub.net/blockchain-glossary/](http://blockchainhub.net/blockchain-glossary/)> (all last accessed 4 July 2019).

scholarship found that it resulted in further confusing regulators.<sup>71</sup> Notably, it leads to the overestimation of the virtues of blockchain, or their actual scope.<sup>72</sup> With regard to blockchain-based decentralisation, it was particularly found to prevent observers from seeing that blockchain networks' governance is often *de facto* less decentralised than promoted, to the benefit of the unaccountable but actual managers of the said blockchain network.<sup>73</sup>

To give a taste of the issue with regard to decentralised applications and entities, it can be observed that, although extensively promoted and discussed within the blockchain community and scholarship, the definition of a “DAO” is not yet settled.<sup>74</sup> The concept of the “autonomy” of a decentralised entity – core to its “trustless trust” virtues – is particularly subject to controversy. *Inter alia*, the degree of autonomy required to be considered genuinely “autonomous” is not clearly settled. As an illustration, “TheDAO”<sup>75</sup> is mostly referred to as the main life example of a DAO; however De Filippi and Wright classify it as a mere DO for lack of sufficient autonomy.<sup>76</sup> As part of this debate, the technical means by which such autonomy is to be acquired is not clear, namely whether artificial intelligence shall necessarily be involved or not.<sup>77</sup> Although the definition of a Dapp by Johnston et al is relatively unchallenged and massively reused, it also leaves numerous questions unanswered. Should the State of the DApps have genuinely tried to conduct due diligence analysis of alleged Dapps, it would have bumped into questions of some importance, such as: does qualification as a Dapp prevent an application from being run by a legal entity at all? In relation thereto, what involvement of the “users” on the changes to the protocol is considered sufficient to qualify as “decision by consensus”? With reference to the application’s “data and records of operation” to be stored on a public blockchain, what exactly shall be “on” blockchain is also unclear. For instance, the Dapp OpenBazaar was found not to “use a blockchain for its core architecture”:<sup>78</sup> can it nevertheless qualify as a Dapp? The list of questions goes on.

The lack of clarity in blockchain vocabulary obviously makes it difficult for users to ascertain what and who they are dealing with when transacting with blockchain-based decentralised applications or entities. Ultimately, where a website claims to be a Dapp, what does it actually claim to be and provide? If a website – say

<sup>71</sup> Walch, *supra*, note 69, 11–13.

<sup>72</sup> MIK, *supra*, note 34, pp 7–9.

<sup>73</sup> Atzori, *supra*, note 6, p 58; A Walch, “In Code(Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains” in P Hacker et al, *Regulating Blockchain: Political and Legal Challenges* (Oxford University Press forthcoming).

<sup>74</sup> Among other stumbling blocks, some consider a DAO as an egalitarian entity, see N Diallo et al, “EGov-DAO: A Better Government Using Blockchain Based Decentralized Autonomous Organization”, *2018 International Conference on eDemocracy eGovernment (ICEDEG)* (2018) p 167.

<sup>75</sup> The DAO was “one of the first decentralized venture capital organizations deployed on the Ethereum blockchain” and its operation, instead of being traditionally delegated to a management team, was “defined using smart contract code”: De Filippi and Wright, *supra*, note 8, p 137.

<sup>76</sup> *ibid*, p 146.

<sup>77</sup> While Atzori considers that DAOs are “self-sufficient agents derived from artificial intelligence” (Atzori, *supra*, note 6, p 46), De Filippi and Wright consider that a DAO may gain its autonomy not only from artificial intelligence, but also from “the aggregation of several code-based systems, which for a larger coordinated system” or in other words by “stigmergic process”: De Filippi and Wright, *supra*, note 8, p 149.

<sup>78</sup> Kaal and Calcaterra, *supra*, note 18, p 19.

CryptoKitties – claims to be a Dapp as part of its blockchain marketing while the definition of a Dapp is not settled, it obviously also makes it harder for users to lodge a complaint arguing that they were illegitimately deceived. In that sense, blockchain vocabulary – and especially the taxonomy of blockchain-based decentralised entities – does not provide appropriate signals for users to help them cope with the imbalance of information that they suffer vis-à-vis blockchain developers. On the contrary, it worsens it by bringing an additional layer of uncertainty or potential malicious use.

This section has demonstrated that the blockchain environment is unable to provide what we termed “meta-trust” with regard to decentralised applications and entities. In other words, blockchain technology may make it possible for A and B to exchange without trusting each other, based on C blockchain-based application; however, blockchain tools are unfit to provide trust to A and B that C application is indeed “trustlessly trustable”. Against this background, we now need to deduce from the above what is needed in order to bring this absent meta-trust into being, with a view to how the law could play a role in this regard.

#### IV. THE ROLE OF THE LAW

Two factors in the blockchain environment have specifically been pointed at as potential tools to bring meta-trust, and have eventually proved to result in the opposite effect: the vocabulary that has emerged in the blockchain environment and especially the taxonomy of blockchain-based decentralised entities on the one hand, and the upsurge of websites serving as (unreliable) directories of the latest on the other hand. The mere conclusion that blockchain vocabulary is vague does not suffice to understand why it is not helpful to bring trust and even why it is so detrimental. After all, legal provisions are also often vague or even unclear; just think of terms largely used in different jurisdictions around the globe such as “reasonable”, “fairness” or “negligence”. How can they nonetheless be entrusted with any value and meaning? The answer is quite obvious: because they are further clarified by judicial authorities, which grant them binding and enforceable interpretation over a given jurisdiction. It is worth noting that the interpretation of unclear blockchain terms is given by what the scholarship has called “benevolent dictators” with regard to the role played by some individuals in bringing “off-chain governance” of the internal blockchain networks but also of the blockchain environment at large.<sup>79</sup> Illustrative thereof is the “post” of Buterin trying to dispel the blur (what he calls the “Daoism”) around the delineation of the various blockchain structures (DAO, DO, Dapp, smart contract . . .).<sup>80</sup> His quasi-regulatory function in the blockchain community demonstrates the *lack* of actual regulation, while it certainly does not satisfy the regulatory demand. Not to mention that he could simply be inaccurate, he obviously lacks the legitimacy as well as the authority to make his statements exclusive, binding and enforceable. Against this backdrop, blockchain

---

<sup>79</sup> Atzori, *supra*, note 6, p 58.

<sup>80</sup> V Buterin, “DAOs, DACs, DAs and more: an incomplete terminology guide”, 6 May 2014, <[blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/](http://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/)> (last accessed 4 July 2019).

vocabulary, the emergence of directories and the role of “benevolent dictators”<sup>81</sup> appear to constitute a distorted mirror of what legal regulation brings. In other words, they can be interpreted as signs that the law is needed. The remainder of this paper therefore attempts to draw guidelines for how the law could help bring meta-trust.

Werbach invited the legal community to rethink the role of the law in relation to blockchain and especially the deemed “regulation vs innovation” dichotomy. Stating that blockchain needs the law to keep up to its promises, he suggests we should look at *how* the law can help blockchain.<sup>82</sup> Blockchain invites lawyers to get back to the basics of the law: Werbach identified classification – ie the activity of naming things – as a major part of the role of regulation<sup>83</sup> that is of acute importance with regard to new technologies, which blur the understanding of traditional regulatory categories.<sup>84</sup> Classification is not only a first step to trigger the application of some substantive obligations, it also makes sense *per se* in order to bring trust by delineating and authenticating a party or a subject-matter. The obligation for an information society service to disclose his identity as trader – enshrined in the E-Commerce Directive (mentioned above) –not only brings a name: it creates a link between a party and a function (namely trader) enabling the consumer, where available, to hold that party accountable for the activity. Similarly, corporate law aims not only to trigger a certain legal regime to a certain form of company; it primarily enables third parties to authenticate with whom they transact, or – more precisely – *what* they transact with. Transacting with a natural person, a non-profit association or a company obviously makes a difference from the perspective of the third party.

In view of the foregoing, it appears that there is a need for regulatory classification of blockchain-based applications and entities – not to mention the other aspects of blockchain technology – as well as the means to have this classification enforced. To be clear and in line with the identified need for meta-trust, the purpose is not the regulation of blockchain activities (it would not regulate, for instance, how the blockchain-based decentralised applications or entities should operate), but the identification and authentication of blockchain “things”. Although it is therefore without prejudice to the required regulation of blockchain activities, it is not an unrelated topic. Regulating (blockchain) activities inevitably requires the performance of regulatory classification. Even when classification is stand-alone regulation, it has an impact on the regulation of activities. The lack of reliable information on fast-evolving technologies – and therefore the uncertainty surrounding the potential effect of a regulation – has been identified as a major explanation for the pacing problem.<sup>85</sup> In the case of blockchain, it was found that the opacity around the technology was partly due to the vagueness of blockchain vocabulary. Regulatory classification could in some cases be sufficient, because it would demonstrate that the blockchain “thing”

---

<sup>81</sup> For a further explanation of the “benevolent dictatorship” phenomenon, see Atzori, *supra*, note 6.

<sup>82</sup> Werbach, *supra*, note 16, pp 534–549.

<sup>83</sup> *ibid*, p 38.

<sup>84</sup> K Werbach, “The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy” (2017) 69 *Florida Law Review* 887 at p 919.

<sup>85</sup> M Fenwick, WA Kaal and EPM Vermeulen, “Regulation Tomorrow: Strategies for Regulating New Technologies” in T Kono, M Hiscock and A Reich (eds), *Transnational Commercial and Consumer Law: Current Trends in International Business Law* (Springer Singapore 2018).

– “Cryptoduck” as named by Werbach<sup>86</sup> – simply proves to be already regulated or in other words to already fall within a regulatory bucket. In that sense, filling the meta-trust gap would empower users and also regulators, by restoring the information asymmetry, if possible *ex ante* – just as corporate law requires companies to register under a specific legal form before operating. Even more, and subject to the regulatory design, it could shift the burden of proof so that “the blockchain” (although it remains to be seen who and how) would have to prove its alleged virtues.

Any regulatory attempt in this regard would, however, be confronted with at least the following challenges and constraints. Firstly, classification may itself fall into the pacing problem, given the fast pace of blockchain development. Secondly, law-makers may simultaneously want to promote – or at least not prevent – potential positive blockchain innovations.<sup>87</sup> Thirdly, the (alleged) decentralised character of blockchain-based applications and entities makes it difficult to identify which entity(ies) should be subject to regulation. The scholarship has already made clear that decentralisation – to a certain extent – does not mean that no entity can be subject to regulation.<sup>88</sup> A fourth, but related, challenge is the identification of the competent actor(s) to introduce such regulation, as well as where the latter should be positioned in the legal system’s hierarchical structure. The two final challenges at least would depend upon the context and the chosen regulatory purpose.<sup>89</sup> Introducing regulatory classification in the blockchain environment is ambitious and could be performed in various designs and with various scopes. The remainder of this paper merely touches upon a few options.

The most obvious option would seem to be simply to define blockchain terminology in statutory law, which was undertaken by a few US States, especially with regard to the legal recognition of blockchain-based electronic signatures and of smart contracts in e-commerce. The law of Arizona defines “blockchain technology” as “distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger [ . . . ]”. The law derives from it the legal recognition of certain features of the data stored on it, such as the fact that “the data on the ledger [would] provide an uncensored truth”.<sup>90</sup> These statutory provisions, however, illustrate a severe misunderstanding of the operation of blockchain, as summarised by Walch: “if a false piece of data is put on a blockchain ledger, it remains false, regardless of the fact that it appears on the ledger (the garbage in / garbage out idea)”. More generally, she notes that regulation of blockchain by the law-maker can be hindered by the fact that the law-maker does not have sufficient understanding of the technology.<sup>91</sup> Regulation of blockchain vocabulary can therefore rather result in bringing additional confusion to the field,<sup>92</sup> especially given the ever-evolving

<sup>86</sup> Werbach, *supra*, note 16, p 37.

<sup>87</sup> De Filippi and Wright, *supra*, note 8, p 189.

<sup>88</sup> MIK, *supra*, note 34, p 13.

<sup>89</sup> De Filippi and Wright, *supra*, note 8, pp 173–192.

<sup>90</sup> Act of September 21 2006, ch 26, Ariz. Rev. Stat. Ann. § 44-7003 (2006) (amended by 2017 Ariz Sess Laws 2417), <[legiscan.com/AZ/text/HB2417/id/1528949](http://legiscan.com/AZ/text/HB2417/id/1528949)>.

<sup>91</sup> Walch, *supra*, note 69, p 10.

<sup>92</sup> Walch especially hints at the debated feature of “immutability” of blockchain, which has been included in the law of Arizona while the blockchain community still lacks a common understanding of its contours and even of its existence: Walch, *supra*, note 69.

character of this technology. If no specific mechanism is provided for, the issue mainly arises from the fact that the law-maker and the judicial authority would have to make highly technical analyses of an ever-evolving technology, which they are poorly equipped to do. Should this option be chosen for a certain scope, it would be therefore wise to provide specific mechanisms to account for the technicalities of the technology: for instance, a registration system could be set up in order to provide for trust *ex ante* (namely before operation) while the analysis of the compliance of a “blockchain thing” with the statutory definition could be delegated to a body having technical expertise. Finally, regulators should pay attention to the principle of technological neutrality, namely the idea that “the law should not pick technological winners and losers, the law should neither help nor hinder particular types of technological artefacts”.<sup>93</sup> Although not enshrined in EU primary law itself, so that it does not constitute a *legal* obstacle as such in EU law, this principle broadly applied in EU secondary law and referred to in EU ICT policies would *logically* prevent the setting up of a techno-specific regulation.

Based on the observation that blockchain is a complex technology based on decentralisation, self-regulation is being undertaken, especially with regard to the classification of blockchain “things” as part of ISO certification.<sup>94</sup> “Dapp”, “DAO” etc could possibly be part of ISO certification. Certification indeed allows terms to be defined according to standards with authority, certified by external knowledgeable bodies. Displaying the respective ISO standard sign on a website alleging its “Dapp” or “DAO” character could therefore bring trust to users, while the question of “who” would display the sign would be partly left up to the internal organisation of the decentralised entity. ISO certification is voluntary and it is beyond legal expertise to try and guess whether the market would broadly embrace certification. Although the existence of (ISO) standards would help users prove the existence and nature of unfair commercial practices (discussed above), for example, it would not prevent *per se* other parties from continuing to promote (alleged) virtues of their blockchain-based decentralised applications or entities. In other words, wrongly claiming to be ISO-certified could be sanctioned,<sup>95</sup> but the use of certified terms – eg Dapp – would remain free for use.

In order to achieve legal certainty while acknowledging the complexity and the decentralised feature of blockchain, co-regulation has been called for.<sup>96</sup> With a view to bringing trust into blockchain terminology, it is hereby suggested that certification be taken a step further, by leveraging “certification marks” recently created in EU

---

<sup>93</sup> The principle of technological neutrality particularly applies in electronic communications law, in the E-Commerce Directive and in the GDPR. See M Thompson, “The Neutralization of Harmony: The Problem of Technological Neutrality, East and West” (2012) 18 Boston University Journal of Science & Technology Law 303. The reach and scope of technological neutrality in ICT policies are however subject to controversy, see C Reed, “Taking Sides on Technology Neutrality” (2007) 4 SCRIPTed 263.

<sup>94</sup> See <[www.iso.org/committee/6266604.html](http://www.iso.org/committee/6266604.html)> (last accessed 4 July 2019).

<sup>95</sup> It could particularly constitute misleading action within the meaning of Unfair Commercial Practices Directive, Art 6(2)(b).

<sup>96</sup> Finck, *supra*, note 4, p 686.



law.<sup>97</sup> Unlike other trademarks which mainly “aim to distinguish the origin of goods and services”,<sup>98</sup> the certification mark has a guarantee function.<sup>99</sup> “Applied for and [...] capable of distinguishing goods or services which are certified by the proprietor of the mark in respect of [*inter alia*] the quality or other characteristics”,<sup>100</sup> the certification mark could guarantee the criteria for qualifying as a Dapp. The certification mark allows<sup>101</sup> and even *requires*<sup>102</sup> the proprietor<sup>103</sup> – eg a certifying body – to prevent non-authorised third parties from using the mark (eg the “Dapp” sign(s)).<sup>104</sup> Contrary to collective marks, the use of certification marks does not have to be limited to a closed group of members. Subject to the provisions of the regulation governing the use of the mark,<sup>105</sup> an “‘open shop’ principle applies”,<sup>106</sup> which fits the open nature of blockchain initiatives. With minimal coordination effort, the certification mark could be used to monitor and sanction the use of the “Dapp” sign by applications wrongly self-advertised as Dapps.

## V. CONCLUSION

Blockchain technology may make it possible to do away with trust in third parties. Yet, as this study of real-life Dapps has showed, this is not enough. The need for trust does not disappear with the arrival of blockchain. Users also need to authenticate (trust) that an alleged Dapp genuinely is one. We have termed this meta-trust, which the blockchain technology and “community” at large were found unable to deliver. Beyond Dapps as a case study, it is argued that blockchain needs the *complementary role of the law* in order to deliver its promises, and especially to authenticate blockchain “virtues”. The article ultimately identified the new EU certification mark as a promising form of co-regulation for that purpose. Failing to find an appropriate mix between the respective operations of blockchain and the law, the article contends that the beneficial innovations expected from public blockchains will not materialise *for the general public* or may shortly fade away. The lack of meta-trust in the blockchain environment would indeed likely result in adverse selection and would have a chilling effect on the acceptance of blockchain innovations.

---

<sup>97</sup> Regulation (EU) 2017/1001 on the European Union trade mark [2017] OJ L 154/1 (European Union Trade Mark Regulation), section 2 of chapter VIII.

<sup>98</sup> A Ringelmann and S Martin, “Defining the EU Certification Mark” (2018) 13 Journal of Intellectual Property Law & Practice 625 at p 626.

<sup>99</sup> *ibid*, p 627.

<sup>100</sup> European Union Trade Mark Regulation, Art 83(1).

<sup>101</sup> *ibid*, Art 90.

<sup>102</sup> *ibid*, Art 91(b).

<sup>103</sup> *ibid*, Art 83(2).

<sup>104</sup> *ibid*, Art 84(2).

<sup>105</sup> *ibid*, Art 84(1); Ringelmann and Martin, *supra*, note 98, pp 628–629.

<sup>106</sup> M Repas and T Keresteš, “The Certification Mark as a New EU-Wide Industrial Property Right” (2018) 49(3) International Review of Intellectual Property and Competition Law 299 at p 303.