European Review of Private Law 6-2019 [825–852]

Blockchain & Data Protection … and Why They Are Not on a Collision Course

Lokke MOEREL*

Abstract: *Recent publications on the data protection aspects of blockchain technology focus on the characteristics of the initial public (Bitcoin) blockchain, and do so in a generalized manner. The authors then conclude that the characteristics of a public blockchain are profoundly incompatible at a conceptual level with the principles of the EU General Data Protection Regulation (GDPR). The GDPR requires identification of a central 'controller' who is responsible for compliance with the GDPR, while a public blockchain decentralizes the storage and processing of personal data, as a result whereof there is no such central point of control. For lack of a better alternative, the authors conclude that all 'nodes' involved in operating a blockchain qualify as a controller under the GDPR, raising enforcement and jurisdictional issues that make it impossible for individuals to enforce their rights. The transparency and immutability of a public blockchain would further not sit well with principles of data confidentiality, data minimization, data accuracy and the rights of individuals to correction and deletion of their data.*

I disagree with the analysis of these authors for a host of different reasons, the main one being that the authors focus on the shortcomings of the initial public (Bitcoin) blockchain when already many new types of permissioned private and consortium blockchain have been developed that significantly diverge from the original, permissionless public blockchain. In fact, these types of permissioned blockchain have been developed in response to the shortcomings of public blockchain. The authors further consider the data processing implications of blockchain as if this technology

* Professor of Global ICT Law at Tilburg University and Senior of Counsel at Morrison & Foerster in Berlin. Ms MOEREL thanks Marijn STORM and Cristina DIACONU for their assistance with research and footnotes. The final version of this contribution was submitted on 6 September 2018. Email: LMoerel@mofo.com.

The irreversibility and transparency of public blockchains mean that they are probably unsuitable for personal data.

Open Data Institute, 2016.[1]

1 J. SMITH, J. TENNISON, P. WELLS, J. FAWCETT & S. HARRISON, 'Applying blockchain technology in global data infrastructure', in Technical Report, *Open Data Institute* (2016), p 16, theodi.org/article/applying-blockchain-technology-in-global-data-infrastructure/ (last visited 18 November 2018); V. LEMIEUX, 'In blockchain we trust? Blockchain technology for identity management and privacy protection,' *Conference for E-Democracy and Open Government* (2017), pp 57-62, https://perma.cc/46D3-WKKK (last visited 18 November 2018); R. NEISSE, G. STERI & I. NAI-FOVINO, 'A Blockchain-based Approach for Data Accountability and Provenance Tracking', *European Commission Joint Research Centre (JRC)* (2017), arXiv:1706.04507 (last visited 18 November 2018); U. ROTH, 'Blockchain Ensures Transparency in Personal Data Usage: Being Ready for the New EU General Data Protection Regulation,' in Special Theme: Blockchain Engineering, *ERCIM News 110* (July 2017), p 32.

constitutes in itself a data processing activity for which a controller has to be identified. Controllership is, however, decided based on a specific use or deployment of a certain technology. Blockchain, like the internet, is a general-purpose technology that is subsequently deployed by actors for a certain purpose in a specific context. Applying the question of controllership to the internet at large would pose similar data protection issues under the GDPR as identified by the authors in respect of blockchain. This publication explains why none of these issues are currently hampering application of the GDPR to the internet and are equally unlikely to pose issues for blockchain applications. This publication describes the issues in their broader context, as well as how each of these issues can be addressed to ensure compliance with the GDPR. The conclusion is that the GDPR is also well able to regulate this new technology. This does not, however, mean that blockchain will thus be suitable for all use and deployment cases.

Résumé: *De récentes publications sur les aspects de la protection des données de la technologie de la blockchain se concentrent sur les caractéristiques de la première blockchain publique (Bitcoin), et le font ainsi d'une manière généralisée. Les auteurs concluent alors que les caractéristiques d'une blockchain publique sont profondément incompatibles à un niveau conceptuel avec les principes du Règlement Général de l'UE sur la Protection des Données (RGPD). Le RGPD exige une identification d'un 'contrôleur' central responsable de la conformité avec le RGPD, alors que la blockchain publique décentralise le stockage et le traitement de données personnelles, de telle sorte qu'il n'y a pas de tel point central de contrôle. Etant donné l'inexistence d'une meilleure alternative, les auteurs concluent que tous les 'noeuds' concernés dans le fonctionnement d'une blockchain sont considérés comme contrôleur selon le RGPD, soulevant des problèmes d'application et de compétence juridictionnelle qui empêchent des individus d'appliquer leurs droits. De plus, la transparence et l'immuabilité d'une blockchain publique ne s'accorderaient pas avec les principes de confidentialité des données, de minimisation des données, d'exactitude des données et les droits des individus à corriger et supprimer leurs données.*

Je ne suis pas d'accord avec l'analyse de ces auteurs pour plusieurs raisons, la principale étant que les auteurs se concentrent sur les lacunes de la première blockchain publique (Bitcoin) alors que se sont déjà développées de nombreuses blockchains privées et de consortium, autorisées, qui divergent de manière significative de la première blockchain publique non autorisée. En réalité, ces types de blockchains autorisées se sont développées en réaction aux lacunes des blockchains publiques. De plus, les auteurs considèrent les implications du traitement des données de la blockchain comme si cette technologie constitue en elle-même une activité de traitement de données pour laquelle un contrôleur doit être identifié. Le contrôle est toutefois décidé sur base d'un usage spécifique ou du déploiement d'une certaine technologie. Une blockchain, comme l'internet, est une techonologie à but général qui est ensuite déployée par des acteurs dans un certain but et dans un contexte spécifique. Appliquer la question du contrôle dans son ensemble à l'internet poserait des questions similaires de protection des données selon le RGPD comme les auteurs l'ont identifié à propos de la blockchain. Cette publication explique pourquoi aucune des ces questions n'entravent actuellement l'application du RGPD à l'internet et de même ne devraient pas poser de problèmes pour des applications de blockchains. Cette publication décrit les questions dans leur contexte plus large et comment chacune de ces questions peut être abordée pour assurer la conformité avec le RGPD. La conclusion est que le RGPD est également tout à fait capable de réglementer cette nouvelle technologie. Cela ne

signifie pas cependant que la blockchain conviendra à tous les cas d'utilisation et de déploiement.

Zusammenfassung: *Die jüngsten Veröffentlichungen zu Datenschutzproblemen der Blockchain-Technologie konzentrieren sich auf die Eigenschaften der anfänglichen öffentlichen (Bitcoin) Blockchain und tun dies in einer allgemeinen Art und Weise. Die Autoren kommen dann zu dem Schluss, dass die Charakteristika einer öffentlichen Blockchain auf konzeptioneller Ebene mit den Grundsätzen der europäischen Datenschutzgrundverordnung (DSGVO) zutiefst unvereinbar sind. Die DSGVO verlangt die Bestimmung einer zentralen für die [...] Datenverarbeitung als verantwortlich zugeteilten[...] Stelle (Controller), die für die Einhaltung der DSGVO verantwortlich ist, während eine öffentliche Blockchain die Speicherung und Verarbeitung personenbezogener Daten dezentralisiert, wodurch es keinen solchen zentralen Kontrollpunkt gibt. Aus Mangel an einer besserer Alternative kommen die Autoren zu dem Schluss, dass alle '*dezentralisierten Punkte*', die am Betrieb einer Blockchain beteiligt sind, als Controller gemäß DSGVO zu qualifizieren sind, was Probleme bezüglich Durchsetzung und Jurisdiktion aufwirft, die es dem Einzelnen unmöglich machen, seine Rechte durchzusetzen. Die Transparenz und Unveränderlichkeit einer öffentlichen Blockchain würde weiter nicht im Einklang mit den Prinzipien von Datenschutz, Datenminimierung, Datengenauigkeit und den Rechten des Einzelnen auf Berichtigung und Löschung seiner Daten stehen.*

Ich bin mit der Analyse dieser Autoren aus einer Vielzahl von verschiedenen Gründen nicht einverstanden, wobei der Hauptgrund darin besteht, dass sich die Autoren auf die Unzulänglichkeiten der anfänglichen öffentlichen (Bitcoin) Blockchain konzentrieren, während bereits viele neue Arten von privaten und Konsortiums-Blockchains mit genehmigten Netzwerk entwickelt wurden, die sich deutlich von der ursprünglichen, öffentlichen Blockchain ohne ein solches unterscheiden. Tatsächlich wurden diese Arten der Blockchain mit genehmigtem Netzwerk als Reaktion auf die Mängel der öffentlichen Blockchain entwickelt. Die Autoren betrachten die Implikationen der Datenverarbeitung bei Blockchain ferner in einer Art und Weise, als ob diese Technologie eine Datenverarbeitungsaktivität in sich selbst darstellen würde, für die ein Controller identifiziert werden muss. Die Kontrollposition wird jedoch auf der Grundlage einer spezifischen Nutzung oder des Einsatzes einer bestimmten Technologie bestimmt. Blockchain ist, wie das Internet, eine Technologie für allgemeine Zwecke, die anschließend von Akteuren für einen bestimmten Zweck in einem bestimmten Kontext eingesetzt wird.

Würde man die Frage nach einer für die [...] Datenverarbeitung als verantwortlich zugeteilten[...] Stelle auf das Internet im Allgemeinen anwenden, würden ähnliche Datenschutzprobleme hinsichtlich der DSGVO aufgeworfen werden, wie sie von den Autoren in Bezug auf Blockchain benannt werden. Dieser Beitrag erklärt, warum keines dieser Probleme derzeit die Anwendung der DSGVO auf das Internet behindert und es ebenso unwahrscheinlich ist, dass Probleme für Blockchain-Anwendungen entstehen. Der Beitrag beschreibt die Problemstellungen in einem größeren Kontext und wie jedes dieser Probleme adressiert werden könnte, um die Einhaltung der DSGVO zu gewährleisten. Das Fazit: Die DSGVO ist ebenso geeignet, diese neue Technologie zu regulieren. Nichtsdestotrotz bedeutet dies aber nicht, dass Blockchain somit für alle Nutzungen und Einsatzoptionen geeignet sein wird.

1. Introduction

1. Despite the fact that blockchain technology (BC)[2] is not yet widely deployed, we have already seen quite some publications about the data protection issues raised by BC. Initially, these publications touted the promise of BC increasing privacy protection by, e.g. facilitating decentralized identity management, allowing the sharing of data with trusted third parties only and presenting a new solution for cross-border data transfers, potentially replacing current contractual solutions, such as the EC Standard Contractual Clauses.[3] In a second wave of publications, we saw a more in-depth discussion of the data protection issues raised by this new technology, generally concluding that *public* BC[4] features are 'on a collision course with EU privacy law,'[5] are 'profoundly incompatible at a conceptual level'[6] with the privacy protection principles of the EU General Data Protection Regulation (GDPR),[7] or in any event 'that it remains to be seen whether EU

2 In this article I will use the narrower term of BC rather than distributed ledger technology (DLT), for reasons of readability, acknowledging that there are other forms of DLT to which this article would equally apply.

3 M. Mainelli, 'Blockchain Will Help Us Prove Our Identities in a Digital World', *Harvard Business Review* (2017), hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world (last visited 18 November 2018); G. Zyskind, O. Nathan & A. Pentland, 'Decentralizing Privacy: Using Blockchain to Protect Personal Data', *IEEE CS Security and Privacy Workshops* (2015), https://ieeexplore.ieee.org/document/7163223 (last visited 18 November 2018); S. Sater, 'Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows', *Tulane University* (2017), papers.ssrn.com/sol3/papers.cfm?abstract_id=3080987 (last visited 18 November 2018); D. Connor-Green, 'Blockchain in Healthcare Data', 21. *Intell. Prop & Tech. L. J.* 93 (2017); A. Tobin & D. Reed, 'The Inevitable Rise of Self-Sovereign Identity', *Sovrin Foundation 1* (29 September 2016, as updated on 28 March 2017), https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (last visited 18 November 2018).

4 There are broadly three categories of BC: private, consortium and public BC. *Private BC* is maintained by a limited number of network nodes belonging to an organization. Read rights can be granted to computers that belong to the network, or could also be granted to selected external computers. *Consortium BC* is generally used by a number of different organizations belonging to a consortium, and involves nodes of the relevant organizations only; here, also, read rights can be controlled. *Public BC* may involve any computer that opts to be a network node and can read/write the BC. Examples of the latter are Bitcoin or Ethereum. Another distinction is between permissioned and permissionless BC: permissioned BC is open to pre-defined subjects only and permissionless BC allows all those with the necessary technical capacity to take part. Private and consortium BC are mostly (but not necessarily) permissioned BC, and public BC is mostly permissionless.

5 D. Meyer, 'Blockchain technology is on collision course with EU privacy law', *IAPP* (2018), iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/ (last visited 18 November 2018).

6 M. Finck, 'Blockchains and data protection in the European Union', *Max Planck Institute for Innovation and Competition Research Paper (MPI Paper) No. 18-01* (2017), p 1.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj (last visited 18 November 2018).

data protection laws can embrace this development'.[8] One author even concludes that there is 'the risk that data protection legislation renders the operation of blockchains unlawful, hence asphyxiating the development of an innovative technology with much promise for the Digital Single Market'.[9] Indeed, the current conception amongst industry stakeholders is that BC is not compatible with the GDPR, resulting in a call for urgent revision.[10] These concerns are fed by public statements of, for example, Jan-Philipp Albrecht (the MEP responsible for coordinating the Parliament's input for the GDPR), that the GDPR requires that individuals can delete their data and that 'this is where blockchain applications will run into problems and will probably not be GDPR compliant', and that therefore blockchain 'probably cannot be used for the processing of personal data'.[11]

1.1. Difficulty to Identify the Controller

2. The main issue raised by the authors[12] is that the GDPR hinges on the notion of a 'controller,'[13] who (alone or jointly with others) is responsible for compliance with the GDPR, in particular for implementation of *privacy-by-design* principles[14] in BC and being the addressee of requests and claims of data subjects.[15] In the current platform economy (with large intermediaries such as Google, Amazon, Apple and Facebook

8 M. Berberich & M. Steiner, 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?', in 2. *European Data Protection Law Review* (2016), p 426.

9 M. Finck, *MPI Paper* (2017), pp 1-2.

10 See D. Meyer, *IAPP* (2018), for a number of quotes from stakeholders voicing concerns that BC is incompatible with the GDPR, that the GDPR is therefore already out of date and therefore already needs urgent revision; see in similar vein (and with similar quotes) also S. Ward, 'Blockchain to Clash with New EU Privacy Law' (2018), www.bestvpn.com/privacy-news/blockchain-clash-new-eu-privacy-law (last visited 18 November 2018); and O. Avan-Nomayo, 'Parity forced to shut down ICO passport service (Picops) due to GDPR' (2018), bitcoinist.com/parity-forced-to-shut-down-picops-due-to-gdpr/ (last visited 18 November 2018).

11 See for quotes Albrecht: D. Meyer, *IAPP* (2018).

12 The authors all also discuss whether the data stored on the BC qualifies as personal data under the GDPR but generally conclude that the GDPR applies to the processing of personal data stored on the BC also if pseudonymized, encrypted or hashed. This is a correct conclusion, as these measures all concern measures that mitigate the impact on the privacy of individuals rather than fully anonymize the personal data that would bring these data outside the scope of applicability of the GDPR, see Art. 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, p 20. For reasons of space, I will refrain from discussing these issues here. See for the conclusion that GDPR applies, M. Finck, *MPI Paper* (2017), p 16 and M. Berberich & M. Steiner, *EDPLR* (2016), p 424; and C. Wirth & M. Kolain, 'Privacy by BlockChain Design: A Blockhain-enabled GDPR-compliant Approach for Handling Personal Data', *Reports of the European Society for Socially Embedded Technologies* 2018, dx.doi.org/10.18420/blockchain2018_03, pp 4-5 (last visited 18 November 2018).

13 The entity that, alone or jointly with others, determines the purposes and means of the data processing (Art. 4 GDPR).

14 Art. 25 GDPR.

15 See for rights of data subjects Arts 12-22 GDPR.

centrally collecting and processing data),[16] it would often be possible to identify *the* entity that is the controller. With BC, there would often not be a central point of control, as *public* BC[17] dispenses with the need for intermediaries, as these are developed as open peer-to-peer systems for everyone to participate in and to effectuate trusted transactions with unknown counterparties.[18] In such set-up, it would be difficult to identify *the* controller. The authors subsequently focus on the role and function of the 'nodes,'[19] mentioning that a public BC is operated by all nodes in a decentralized fashion. The conclusion of the authors is that for these BC, either no node would qualify as a controller (with the result that no controller could be identified at all, which cannot be the case, as the requirements of the GDPR would not apply at all), or every node would qualify as such.[20] The authors then conclude that, by lacking a better alternative, the conclusion has to be that each node qualifies as a controller and that therefore data subjects can invoke claims against each node independently.[21]

The authors indicate that this may be different in case of private or a consortium BC (permissioned BC operated by one organization or a consortium of organizations, respectively),[22] as in those cases, it might well be possible to identify a central intermediary that can qualify as the controller, such as the systems operator.[23]

---

16 M. Finck, *MPI Paper* (2017), p 6 describes it as follows: 'the GDPR was fashioned for a world where data is centrally collected, stored and processed, [while] blockchains decentralize each of these processes.' BC would offer a record keeping function that 'dispenses with the need for an intermediary,' which is 'in sharp contrast with the current data economy, characterized by economic centralization in the form of 'platform power'', whereby 'large intermediaries such as Google, Amazon, Apple and Facebook control how we search, shop and connect'.

17 See for description of the various categories of BC, fn 4.

18 M. Finck, *MPI Paper* (2017), p 6 and M. Berberich & M. Steiner, *EDPLR* 2016, p 422.

19 BC is a distributed peer-to-peer ledger stored on every node of the system. If a new transaction is effected, the nodes verify the legitimacy of the effected transaction and, for some BC applications, provide decentral storage for the BC's ledger. Any device with an internet connection can be used as a node but, due to the processing and storage requirements, mostly computers are used as nodes. The node willingly contributes (a part of) its processing or storage abilities to the BC network. Alternatively, some forms of malware transform the device of an unsuspecting user into a node, sapping its processing or storage abilities.

20 M. Finck, *MPI Paper* (2017), p 16 and M. Berberich & M. Steiner, *EDPLR* (2016), p 423.

21 See M. Finck, *MPI Paper* (2017), p 17 for an explanation why it is justified that each node qualifies as a controller: 'nodes are indeed not subject to external instructions, autonomously decide whether to join the chain, and pursue their own objectives (...) it appears that the Regulation's legal obligations would rest on each node, meaning that data subjects can invoke claims via-à-vis each node independently'; see also M. Berberich & M. Steiner, *EDPLR* 2016, p 424; C. Wirth & M. Kolain, *Reports of the European Society for Socially Embedded Technolgies* 2018, p 5, under reference to M. Martini & Q. Weinzierl, 'Die Blockchain-Technologie und das Recht auf Vergessenwerden', *Neue Zeitschrift für Verwaltungsrecht (NVwZ)* 2017, pp 1251–1259.

22 See for description of distinctions between different BC, fn 4.

23 M. Finck, *MPI Paper* (2017), p 16 and M. Berberich & M. Steiner, *EDPLR* (2016), p 424.

3. Consideration is subsequently given to the question whether all nodes together could qualify as joint-controllers, but this is generally rejected as these nodes 'do not jointly determine the purposes and means of the processing.'[24] Also considered is whether individuals could qualify as controllers themselves when they decide to use BC for a certain transaction, whereby the individual would both be a data subject as a data controller. This issue is raised but not discussed 'as it would turn the conceptual GDPR framework on its head'.[25]

2. Overview Issues Posed by BC Under the GDPR

4. The publications subsequently discuss all the issues and complications raised under the GDPR if each and every node qualifies as a controller:

- **Jurisdiction and enforcement.** Enforcement for Data Protection Authorities (**DPAs**) and data subjects would be difficult, as it is difficult to determine the exact number, location and identity of the nodes;
  As one author describes it:[26]

  For the Bitcoin blockchain, there are currently approximately 11,000 nodes around the planet, of which about 1800 are in Germany and 800 in France. If one were to address each of these nodes, some of which may not be found, in a single jurisdiction this would create two sets of problems. First, a large amount of nodes would need to be contacted and compelled to comply, as opposed to a single controller in a data silo scenario. Second, this may lead to forcing all nodes to stop running the blockchain software, where GDPR rights cannot be achieved through alternative means.

- **Rights of individuals of access, correction and deletion.** Nodes often only see the encrypted or hashed form of the data and are unable to make changes thereto, and therefore they cannot respond to the tasks the GDPR requires of the controller, such as providing data subjects with access to their data and to correct or delete their data where required. Due to the immutability of the BC, BC is, by definition,

---

24 See M. Finck, *MPI Paper* (2017), p 17; C. Wirth & M. Kolain, *Reports of the European Society for Socially Embedded Technologies* (2018), p 5, under reference to R. BÄUHME & P. Pesch, 'Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie', *Datenschutz und Datensicherheit (DuD)*, pp 473-481

25 M. Finck, *MPI Paper* (2017), p 17. Other than how this is represented by Finck, this seems to me an old issue that has already been extensively raised and discussed in respect of for instance social media networks. See on this in detail paragraph 4.8.

26 M. Finck, *MPI Paper* (2017), p 17.

unable to forget, as a result of which the right to be forgotten will be impossible to enforce;[27]

- **Data accuracy and data minimization.** The immutability of BC runs further contrary to the principles of data minimization and storage limitation. These principles require that controllers keep data up-to-date and do not process more data than required to fulfill the relevant purpose and also not retain such data longer than required for such use.[28] This requires that data are deleted or corrected when no longer accurate, that retention periods are defined and that the data are deleted once such retention periods expire.
- **Confidentiality.** Public BC is an open system in which all data on the BC are available to all nodes. This means that, by definition, the nature of public BC is at odds with the GDPR's principle of confidentiality, which requires that access to data is only provided on a 'need to know' basis.[29]

3. A different Perspective – BC in Context

5. I do not agree with the analysis in these initial publications for a host of different reasons. Before I discuss the GDPR issues raised in respect of deployment of BC in more detail, I will first give a broader perspective on BC as a new technology and the potential governance issues relating thereto.

3.1. BC is a General Purpose Technology

6. BC, like the internet, is a general purpose technology,[30] which is subsequently deployed by actors for a certain purpose in a specific context. The authors, however, consider the data processing implications of BC as if the technology in itself constitutes a data processing activity for which a controller has to be identified. This is a similar exercise as if we would attempt to identify in general who the controller is in respect of the entirety of data processing via the internet or via

27 M. Finck, *MPI Paper* (2017), pp 20–24 and M. Berberich & M. Steiner, *EDPLR* (2016), p 426.

28 M. Finck, *MPI Paper* (2017), p 20 and M. Berberich & M. Steiner, *EDPLR* (2016), pp 424–425.

29 DIGITAL ASSET PLATFORM, *Non-technical White Paper* (2016), bit.ly/2mmwje7, p 7 (last visited 18 November 2018); See also R. Ribitzki et al., 'Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare', *Blockchain in Healthcare Today* (2018), p 3.

30 D. Tapscott & A. Tapscott, 'Realizing the Potential of Blockchain, A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies', in White Paper, *World Economic Forum* (2017), www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf, p 31 (last visited 18 November 2018). See also W. Drake, V. Cerf & W. Kleinwächter, 'Internet Fragmentation: An Overview', in Future of the Internet Initiative White Paper, *World Economic Forum* (January 2016), p 11.

email functionality. This is not a useful exercise. Everybody understands intuitively that it is impossible to identify one controller in respect of the internet or in respect of all emails sent via email functionality. Controllership is decided based on a specific use or deployment of a certain technology, not in respect of technologies in general. Applying the question of controllership to the internet at large would result in a similar conundrum as when applied to public BC: either all technical building blocks of the internet would qualify as a controller or none of them would, a result that would pose similar data protection issues under the GDPR as identified by the authors in respect of BC. None of these issues have, however, hampered the development of the internet, for the simple reason that controllership is not decided based on the technical level of operation of the relevant technology, but is based on who deploys this technology for a certain purpose. For example, a website owner uses the internet to offer its website. It is the website owner who qualifies as the controller in respect of the processing of any personal data via the website and not the operator of the technical infrastructure. Below, I will explain why application of EU data protection laws has not hampered the development of the internet and will equally likely not pose issues for BC.

3.2. BC as a new Global Resource

7. The character and potential of BC is well described by the World Economic Forum Report 2017 on BC (WEF Report).[31] The WEF Report describes BC as a *new global resource*[32] like the internet, that requires *global stewardship*:[33]

> The few last decades brought us the internet of information. We are now witnessing the rise of the internet of value. (...) We can send money and soon any form of digitized value – from stocks and bonds to intellectual property, art, music and even votes – directly and safely between us without going through a bank, a credit-card company, PayPal or Western Union, social network, government or other middleman.

As BC is about *value* rather than 'just' information, BC 'cuts to the core of legacy industries like banking' and also other forms of value like public land registers or trademark registers.[34] As it is about whether someone has ownership of money,

31 D. Tapscott & A. Tapscott, *WEF Report* (2017).

32 D. Tapscott & A. Tapscott, *WEF Report* (2017), p 7: 'So important is this new resource that some have called the blockchain a public utility like the internet, a utility that requires public support'.

33 *Stewardship* involves, according to the authors: 'collaborating, identifying common interests and creating incentives to act on them. We do not mean *government*, which involves legislating and regulating behaviour and punishing those who misbehave'.

34 D. Tapscott & A. Tapscott, *WEF Report* (2017), p 8.

stocks, houses or not (as evidenced by the BC), the participants will insist that their stakes will be safeguarded (also in the long term) before the BC will be trusted. The prediction is therefore that, whenever BC applications are built for evidence and transfer of value, there will always be a set of *governance rules* reflecting the terms agreed by the participants of the eco-system to regulate their relationship, as well as a governance mechanism for agreeing on changes thereto going forward.[35] The result thereof will be that if a party participates as a member in this eco-system, the rules of the platform will apply.

3.3. No Longer any Middlemen?

8. The authors discussing the data protection issues predict that, due to the decentralized character of BC the traditional middlemen will become obsolete, such as the authorities that run the public land and trademark registries.[36] However, BC will not make intermediaries obsolete, but it will likely replace the current intermediaries.[37] As the internet disrupted many business models and intermediaries, the BC will in turn likely disrupt and replace even these new intermediaries with yet new intermediaries. As new BC business models are just emerging, it is difficult to foretell exactly what these intermediaries will look like. The first examples,[38] however, show that new intermediaries are indeed materializing, either as a single entity or as a consortium of entities (often comprising of or being funded by incumbrants, such as financial institutions), which intermediaries are in charge of the governance of the BC platform or the entities operating a BC *application* on top of the BC platform for specific eco-systems.[39] These

35 D. Tapscott & A. Tapscott, *WEF Report* (2017), p 9: 'It illustrates the profound differences between managing information creation versus value creation activities. The latter require deep negotiation, contractual and jurisdictional understandings, and the ongoing stewardship of application-level ecosystems.' This may well be in the form of 'membership rules' governing the decentralized organization, see P. de Filippi & A. Wright, 'Decentralized Blockchain technology and the Rise of Lex Cryptographia', *Socials Sciences Research Network* (10 March 2015), p 31.

36 M. Finck, *MPI Paper* (2017), p 6 and M. Berberich & M. Steiner, *EDPLR* (2016), p 422.

37 D. Tapscott & A. Tapscott, *WEF Report* (2017), p 5: 'Of course, this does not mean that middlemen will disappear. Rather the technology provides profound opportunities for innovative companies and institutions in the middle to streamline processes, increase their metabolism, create new value and enter new markets.' and P. de Filippi & A. Wright, *Socials Sciences Research Network* (2015), p 51: 'Even in a world dominated by decentralized data and organizations, powerful intermediary will still remain.'

38 See for an overview of the top 10 cryptocurrencies and a discussion of the set-up and governance of a number of these as well as subsequent governance challenges, D. Tapscott & A. Tapscott, *WEF Report* 2017, pp 10–17. See also p 25 where the challenge is discussed that 'powerful encumbrants will usurp domains' by being the largest investors in BC ventures.

39 D. Tapscott & A. Tapscott, *WEF Report* (2017), pp 8–9, describe that as to BC roughly three levels can be identified where decisions are made. The first is the platform level, the protocols of BCs such as bitcoin, Ethereum, Ripple or Hyperledger. The second is the application level, the tools that run on platforms, tools such as smart contracts, that require massive cooperation between

BC applications are therefore private and consortium BC rather than public BC, both in order to meet business needs as well as to gain social acceptance.[40] These BC applications are further permissioned, in the sense that they implement membership rules, that determine which parties have read or read/write authorization. By controlling read rights, the access to the information on the BC can be limited to those parties that need to know this information. To avoid jurisdictional and enforcement disputes, these rules will also provide who the responsible entity is, as well as a choice of law and forum.[41]

3.4. Cross-Border Enforcement and Jurisdiction Issues?

9. By now many different types of BC are being developed, some of which have been designed for specific purposes or industries, others are more generic. The generalized discussion by the authors on for example the enforcement issues due to the decentralized character of BC, is therefore likely not a realistic reflection of how these issues will be encountered in practice.

As Eliza Mik in her contribution notes:[42]

> [O]nce it is acknowledged that there are different types of blockchains, it becomes clear that in most instances it is impossible to generalize. More specifically, arguments made in the context of permissionless blockchains (such as Bitcoin or Ethereum) lose their validity in the context of permissioned blockchain.

10. Also, here it is well to remember that the early predictions in respect of the internet foresaw similar enforcement and jurisdictional issues.[43] Every encounter of consumers in cyberspace would raise the possibility that diverse laws would apply and multiple courts would have jurisdiction, and a myriad of court cases was predicted.[44] Another early

---

stakeholders to work. The third is potentially the overall ecosystem, the ledger of ledgers connecting (or not) the various BC platforms, such as bitcoin, Ethereum, Ripple and Hyperledger.

40 See Tapscott & Tapscott, 'Realizing the Potential of Blockchain', p 21, indicating that governance is critical to the success of commercial BC applications: 'For example, Ripple's global payments steering group, a blockchain bankers network with defined rules and governance, has been a major step forward in terms of adaption and industry acceptance.'

41 P. Botsford, *International Bar Association* (2017): 'Any blockchain-based application raises potential jurisdictional knots: each transaction could fall under the jurisdiction of the various locations of the network, but this seems unworkable. Instead, parties (or platforms?) in a transaction will establish governing law and jurisdiction clauses to provide greater certainty about what laws would apply.'

42 M. Mik, 'Electronic Platforms: Openness, Transparency & Privacy Issues', p 853.

43 This paragraph draws from one of my earlier publication, where I described online cross-border enforcement issues and how best to regulate these extensively in: L. Moerel, *Binding Corporate Rules, Corporate Self-Regulation of Global Data Transfers*, (Oxford University Press 2012), paras 4.3–4.4.

44 P. Swire, 'Elephants and Mice Revisited: Law and Choice of Law on the Internet', in *University of Pennsylvania Law Review* (vol. 153: 2005, 1975–2001), Ch. 2, fn 72, pp 1991–1992, https://scholarship.law.upenn.edu/penn_law_review/vol153/iss6/4/ (last visited 18 November 2018).

prediction about e-commerce was that search engines and the global reach of the internet would eliminate the need for wholesalers and other intermediaries, which would again give rise to many disputes directly between businesses and consumers.[45]

Contrary to these early expectations, there have been only isolated court cases dealing with online cross-border consumer disputes.[46] One of the mechanisms that explain why so few court cases actually materialized is that stakeholders quickly found practical work-arounds in the form of contractual self-regulatory systems.[47] Examples are the use of credit cards for online payments that bring their own dispute resolution system[48] and the emergence of large intermediaries like eBay, which was at first just regulated by the ratings and review consumers could post, but later introduced full-fledged dispute resolution.[49] Also, here the old

45 P. Swire, *UPLR*, vol. 153 (2005), pp 1991–1992.

46 P. Swire, *UPLR*, vol. 153 (2005), notes that 'Surprisingly, however, the number of actual cases addressing choice of law on the Internet is far, far lower than the initial analysis would suggest. Although there is the possibility of diverse national laws in every Internet encounter, some mysterious mechanisms are reducing the actual conflicts to a handful of cases.'

47 P. Swire, *UPLR*, vol. 153 (2005), p 1976.

48 P. Swire, *UPLR*, vol. 153 (2005), p 1990, gives this as the main reason for the fact that there are so few court cases involving online consumer purchases: '(...) credit card purchases (and systems such as PayPal that are based on credit and debit card accounts) have become the dominant means of payment over the Internet'. As a result '[s]ellers and buyers are subject to the elaborate rules of the credit card payment system, and so there is relatively little recourse to national courts. Credit cards have two decisive consumer protections compared with e-cash systems. If there is unauthorized use of the credit or debit card, the individual's loss is limited by US statute, usually to $50.47. In addition, the credit card brings with it an already-functioning dispute resolution system. If a merchant claims that a customer has spent $200 on software, and the customer disagrees, then the customer is not charged for the $200 while the dispute is in process. With these ready-made ways to protect customers against unauthorized use and to resolve disputes, the credit card system inspires trust in consumers, creates effective dispute resolution mechanisms, and avoids the need for recourse to national courts'.

49 As P. Swire, *UPLR*, Vol. 153 (2005), pp 1991–1992, explains it in respect of the emergence of e-commerce: 'Consumers can feel that it is very risky, however, to buy from a website they have never heard of, in a country far away. One major cure for this problem has been the phenomenal growth of auction sites, especially the Internet intermediary eBay (...). Although it was likely not a major goal of eBay's managers to avoid conflict-of-laws disputes, that has been one effect of the business model. Initially, trust in eBay was supposed to result from feedback ratings that customers gave to each other. Over time, however, eBay has created an entire legal system that accompanies each sale. The system contains at least a dozen consumer protections, including fraud protection for the buyer, an escrow service so that buyers can examine an item before payment goes to the seller, a verified identity program, and a system for fraud enforcement including referrals if necessary for criminal activity. (...) Although eBay initially became famous for small purchases, such as hobbyist collectibles, today's eBay includes numerous auctions for valuable items such as diamonds. Even these large consumer transactions appear to be conducted without recourse to national courts, avoiding judicial pronouncements'.

intermediaries (retailers) were replaced by new intermediaries, generating again the required trust to do business.

11. It is therefore a justified expectation that, due to the lack of government regulated supervision, the stakeholders involved in BC will implement their own contractual self-regulatory mechanisms to ensure adequate dispute resolution, as happened with the internet. In fact, there is very little happening on the internet that is not governed by some form of contract. The use of websites is regulated by their website terms & conditions, online purchases are governed by purchase terms, access to the internet is governed by the terms and conditions of ISPs, App stores have their own T&Cs, search functionality is governed by the T&Cs of the provider of the search engine, etc. As explained above, we already see a similar development with BC, where private and consortium BC implement membership rules to ensure adequate dispute resolution.

12. More in general, I note that also the Internet started out as a fully decentralized network. Based thereon, the expectation of the early pioneers was that the Internet would therefore replace the existing centralized organizations through the distribution of communication tools.[50] The Internet was proclaimed to be a free haven where you could remain anonymous and beyond territorial jurisdiction.[51]

These predictions have again not materialized. In recent years, we have, in fact, seen a radical concentration and centralization of internet services, whereby few large organizations control important hubs on the Internet (the platform economy).[52] Even, governments and companies have by now transformed the Internet into the ultimate apparatus for political and social control by monitoring speech, identifying dissidents and disseminating propaganda.[53]

---

50 De Filippi & Wright, 'Decentralized Blockchain technology', 19-20, under reference to: J. Barlow's, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation* (1996), projects.eff.org/~barlow/Declaration-Final.html (last visited 18 November 2018).

51 See Barlow, 'A Declaration of the Independence of Cyberspace', declaring the Internet to be a 'new home of [the] Mind' in which governments would have no jurisdiction. . This paragraph draws on L. Moerel, 'Big Data Protection, How to Make the Draft EU Regulation on Data Protection Future Proof', *Oratie Universiteit Tilburg* (2014), www.mondaq.com/x/298416/data+protection/Big+Data+Protection+How+To+Make+The+Draft+EU+Regulation+On+Data+Protection+Future+Proof, p 18 (last visited 18 November 2018).

52 De Filippi & Wright, 'Decentralized Blockchain technology', pp 19-20, under reference to: 'While the Internet has liberated information, and contributed to the democratization of markets, it has done little to transform many of the centralized organizations that existed before the dawn of the digital age. Governments and large corporations have in fact grown, as they leveraged the raw distributive power of the Internet.', under reference to J. Goldsmith & T. Wu, *Who Controls the Internet: Illusions of a Borderless World* (Oxford University Press 2006), pp 142-161. See further Zyskind et al., 'Decentralizing Privacy', p 1.

53 L. Moerel, 'Big Data Protection', p 18, under reference to N. Carr, 'The Big Switch, Rewiring the World From Edison to Google' (2013), 242. N. Richards & J. King, 'Three Paradoxes of Big Data',

It is therefore not a given that the second wave of decentralization as promised by BC, will thus result in the level of decentralization assumed by the authors. As governments and companies over time managed to re-centralize and monitor the decentralized Internet, they may well also succeed in again re-centralizing and monitoring BC. It is quite possible (and in my view even likely) that BC will ultimately be used to further increase control over transactions and behaviour of individuals, due to BC being used for central identity management and the permanent recording of every online activity.[54]

13. Again, this may well be different with a public BC, especially those in the B2C context. This is exactly the reason why it is expected that public BC will become regulated by public governments.[55] This seems also the take of Oscar Borgogno in his contribution, who indicates that, for BC applications in the B2C context, 'policy makers and regulators *should take the lead i*n order to guarantee a trustworthy translation into code of consumer contracts.'[56] However, also

---

Stanford Law Review Online 66 (2013), www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data (last visited 18 November 2018), call this the 'power paradox' and give the following example: 'Many Arab Spring protesters and commentators credited social media for helping protesters to organize. But big data sensors and big data pools are predominantly in the hands of powerful intermediary institutions, not ordinary people. Seeming to learn from Arab Spring organizers, the Syrian regime feigned the removal of restrictions on its citizens' Facebook, Twitter, and YouTube usage only to secretly profile, track, and round up dissidents'. Zyskind et al., 'Decentralizing Privacy', p 1.

54 See in the same vein: De Filippi & Wright, 'Decentralized Blockchain technology', p 53: 'The blockchain could be used, for instance, to manage identity, making it easier to monitor, surveil, or simply keep track of various online activities. Every transfer, vote, purchase can be recorded on the blockchain, creating a permanent record that will potentially push the boundaries of privacy law.' In any event, as with the Internet, governments may well find intermediaries to 'hook' on to (such as ISPs), to keep control over the BC ecosystem. See p 51: 'Yet, the blockchain is – and will fundamentally remain – a regulatable technology. While states initially had a hard time grasping how to regulate a global and decentralized network like the Internet, they eventually came to the understanding that, as long as there are centralized chokepoints, regulation can be achieved, through the indirect regulation of the various intermediaries and online operators that actually run the network (...). An analogous situation will likely take place in the context of blockchain technology. Even in a world dominated by decentralized data and organizations, powerful intermediary will still remain. If threatened, states and governmental actors could adopt a series of draconian measures to regulate the emerging online ecosystem and to retain control over the blockchain ecosystem.'

55 See also D. Tapscott & A. Tapscott, *WEF Report 2017*, p 8, where it is predicted that for the internet of value, many societies will expect government to protect the public interest: 'while governments and regulators alone lack the knowledge, resources and mandate to govern this technology effectively, government participation and even regulation will likely have a greater influence over blockchain technologies [*author: than the internet*] to ensure that we preserve both the rights and powers of consumers and citizens.'

56 O. Borgogno, *Smart Contracts as the (new) Power of the Powerless? The Stakes for Consumers and Businesses*, p 885. In respect to the B2B scenario, Borgogno concludes that there 'will *just* be the need for oversight by public bodies'.

public BC in the B2B context may well require public regulation (if not outright prohibition), as we already see that these forms of BC are inherently prone to abuse for criminal activity due to full decentralization and encryption.[57]

3.5. Broader Governance Issues

14. That there will be contractual self-regulatory rules governing an *individual* BC does not take away more general regulatory concerns. As a general purpose technology, BC would benefit for example from global standard setting to ensure the interoperability of BC applications on the various BC platforms as well as to ensure interoperability between the various BC platforms. Below, I will explain that the internet has never been centrally regulated by public institutions, which poses broader *governance* issues. We will very likely encounter similar governance issues with BC. For these broader governance issues lessons can be learned from the current (lack of) central governance of the internet and the emergence of internet governance institutions to fill the gaps in central public governance.[58] It is clear that many find that the lack of comprehensive governance institutions for the internet as a whole has often led to inefficiencies and by now even threaten the open character of the internet.[59] As BC is expected to have a disruptive effect of a magnitude that is at least similar to that of the internet,[60] it is clear that efficiencies could be gained if we would learn from the many governance issues encountered in respect of the internet and would be able to leverage the governance institutes that by now have emerged to deal with these issues.[61]

15. Note, however, that the broader internet governance issues do not make the internet inherently incompatible with the GDPR, just because there is no central controller to be identified for the internet at large. A similar conclusion will apply to BC. We already see new forms of governance and decision making emerge in relation to BC as a general purpose technology (maybe even too many), mostly in forms of multi-stakeholder governance groups.[62]

---

57 See on the potential of abuse of BC for criminal activity: P. DE FILIPPI & A. WRIGHT, *Socials Sciences Research Network* (2015), pp 20–24.

58 See on the development of governance of the internet (and how to balance the demands for national sovereignty and transnational cyberspace) as well as recent governmental fragmentation of the internet W. DRAKE, V. CERF & W. KLEINWÄCHTER, *WEF Report* (2016), pp 31–45.

59 See on the different levels of fragmentation which now threaten the open character of the internet: W. DRAKE, V. CERF & W. KLEINWÄCHTER, *WEF Report* (2016).

60 D. TAPSCOTT & A. TAPSCOTT, *WEF Report* (2017), p 8.

61 See on current governance institutions of the internet, D. TAPSCOTT & A. TAPSCOTT, *WEF Report* (2017), p 7.

62 See for overview of all governance networks that already emerged in respect of BC: D. TAPSCOTT & A. TAPSCOTT, *WEF Report* (2017), at Appendix: Global Solutions Network (pp 36–40).

16. It is clear, however, that any global governance of BC is at the moment very impromptu and opaque, which has the inherent risk that 'informal and invisible power dynamics emerge, often more centralized than they appear.'[63] The governance will therefore require further thinking and may ultimately possibly also require public regulation.[64]

3.6. The GDPR does not Impose Requirements on Designers of Technology

17. The GDPR includes an obligation for the controller to set up data processing functions on the basis of *privacy-by-design.*[65] This requires controllers to mitigate the privacy impact on individuals from the outset, ensuring that their rights are already safeguarded in the *design* of the product or service (ex-ante) rather than that individuals have to enforce their legal rights after the processing has already taken place (ex-post).[66] The GDPR does not require providers of software and infrastructure that are used to process personal data to ensure

---

63 Quote of P. DE FILLIPI in D. TAPSCOTT & A. TAPSCOTT, *WEF Report* (2017), p 8. See also pp 13 and 32. Note that, for each BC, there is, in the end, always a small group of core developers who have developed and set up the BC (also the public BC) and have technical authority to make changes to the BC code, and they do so when specific failures are identified. Example here can be the Ethereum incident, whereby hackers managed to steal 3.6 million of the cryptocurrency Ether (with a total value of about 50 million USD), which led the Ethereum community to agree to a hard-fork splitting up the BC. See on this incident D. TAPSCOTT & A. TAPSCOTT, *WEF Report* (2017), pp 15–17.

64 See for some initial thinking on the societal challenges posed by decentralization and encryption (which are not new but are more difficult to control with BC) and some initial thinking how best to regulated these: P. DE FILIPPI & A. WRIGHT, *Socials Sciences Research Network* (2015), p 18.

65 Art. 25 GDPR. Relevant here is that privacy by design implies that compliance with and enforcement of legal standards is incorporated from the outset into technical designs.

66 This paragraph draws on L. MOEREL & C. PRINS, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (25 May 2016), ssrn.com/abstract=2784123 (last visited 18 November 2018)(translation into English of: '*De Homo Digitalis – Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things*,' published by Wolters Kluwer), pp 10 and 93, under reference to H. NISSENBAUM, 'A Contextual Approach to Privacy Online', Dædalus, *the Journal of the American Academy of Arts & Sciences* (2011), pp 32–48, www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf (last visited 18 November 2018); and O. TENE & J. POLONETSKY, 'Privacy in the Age of Big Data: A Time for Big Decisions', *Stanford Law Review* (vol. 64:63, 2012), para. 1, https://iapp.org/media/presentations/12Summit/S12_De-identification_HANDOUT_1.pdf (last visited 18 November 2018): 'In the context of online privacy, this implies emphasis should be placed less on notice and choice and more on implementing policy decisions with respect to the utility of given business practices and on organizational compliance with fair information principles (FIPs). In other words, the focal point for privacy should shift from users to: (a) policymakers or self-regulatory leaders to determine the contours of accepted practices; and (b) businesses to handle information fairly and responsibly.' See further L. BYGRAVE, 'Hardwiring Privacy', in R.

that their products and services are developed based on privacy-by-design. As a consequence, individual controllers need to expressly instruct each of their technology suppliers to provide software and infrastructure that incorporate privacy-by-design in order to meet the controller's obligations under the GDPR. In other words, the GDPR only *indirectly* regulates the design of technologies, as the controllers deploying the technology will have to ensure that the technology they choose to deploy is compliant with the privacy-by-design principle under the GDPR. At first blush, this seems an ineffective way of regulating. An obvious and simple solution would have been to require software manufacturers to directly design products that are based on privacy-by-design.[67] This provision, however, did not make it into the GDPR.[68] Though this indirect manner of regulating seems inefficient, the reality, however, is that for technology developers, it is often difficult to foresee all possible deployments of their technology. As a consequence, it is difficult to implement all requirements into their product from the outset. It is often in the feedback loop of the users, customers or society at large when the technology is deployed in practice that the design issues become apparent and are addressed. Too-strict upfront design requirements (in the form of standards) may even hamper innovation, and it may even lead to 'widespread adoption of inferior technology.'[69] In the words of Behlendorf (CEO of the Linux Foundation): [70]

> The space is still so young that the desire for standards, while well-placed, runs the risk of hardening projects that have just come out of the lab and we need to avoid making serious architectural decisions that first become legacy and then become a hindrance.

18. In a similar vein, the internet has gained such global presence also *because* it was not subject to upfront regulation from the outset.[71] It is subsequently in each

---

Brownsword, E. Scotford & K. Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press 2017), p 755.

67 This would enable enforcement against the supplier rather than against each and every one of its customers using the relevant software for their data-processing activities. Suppliers generally have no commercial interest in the data collection itself, which may result in a better implementation of the principles of privacy by design than if this is left to data controllers. See L. Moerel & C. Prins, 'Privacy for the Homo Digitalis', p 10.

68 Recital 61 of the GDPR only contains a recommendation to Member States that producers should be 'encouraged' to design their products on the basis of privacy-by-design. To date, we have not seen national governments of the EU to have taken action on this point.

69 D. Tapscott & A. Tapscott, *WEF Report* (2017), p 19.

70 Quote from D. Tapscott & A. Tapscott, *WEF Report* (2017), p 19. The report also notes that having too many BC protocols out there competing for too long, will also hamper further development of BC, as it will be difficult for other parties to build applications that have to run on top of the platform layer.

71 W. Drake, V. Cerf & W. Kleinwächter, *WEF Report* (2016), p 31.

and every use case that the legal requirements have kicked in (whether data protection, e-commerce, consumer protection or otherwise) which have had their impact on the design of many new technologies. This is also evidenced by the fact that by now many basic privacy-by-design requirements have found their way in, for example, standard software design principles.[72,73]

19. Over time, EU data protection laws have shown to be well able to cater for the development of internet related technologies. The GDPR (as was its predecessor the Data Protection Directive) is technology agnostic[74] in the sense that it provides for general data protection principles and requirements but does not prescribe any technology or technical manner how these principles and requirements should be implemented. As BC is an emerging technology still in its infancy, the GDPR works exactly as it is intended, challenging developers to think of creative ways of how to develop the technology in such a manner that the impact on the privacy of individuals can be mitigated and basic principles of the GDPR can be complied with. That this may take some development cycles to be achieved is fully understood.

20. The conclusions of the authors that public BC is at odds with the principles of the GDPR, and that the GDPR is thus unable to embrace this new technology, is missing the point that the GDPR is intended to provide guidance on how to develop new technology in the first place. Also, the conclusion of one author that 'we must be willing to adapt the law to technologic change and accepting of greater techno-legal interoperability'[75] seems off the mark, where the GDPR and the EU data protection supervisory authorities actively stimulate technical-legal interoperability. This is exactly why the principle of privacy-by-design is now codified in the GDPR, as it is well understood that technologic innovations may be able to better effectuate material data protection than any legal rule would ever be able to effectuate in practice (whether due to lack of compliance or otherwise).[76]

---

72 See for example: International Organization For Standardization, 'ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework', iso.org/standard/45123.html (last visited 18 November 2018), Federal Office For Information Security, 'IT Grundschutz Catalogues', bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html (last visited 18 November 2018), and Commission Nationale Informatique & Libertés, 'Security of Personal Data', cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf (last visited 18 November 2018).

73 I note that having too many BC protocols out there competing for too long will also hamper further development of BC, as it will be difficult for other parties to build applications that have to run on top of the platform layer. D. Tapscott & A. Tapscott, *WEF Report* (2017), p 19.

74 Recital 15 of the GDPR.

75 M. Finck, *MPI Paper* (2017), p 2.

76 See on the enforcement issues in respect of the rights of individuals to data protection: L. Moerel, (Oxford University Press 2012), para. 4.3. See on the benefits of privacy-by-design requirements: the literature listed in fn 67. See further B. Brownsword, '*Smart Transactional Technologies, Legal*

3.7. Individuals as Data Subjects and as a Controller

21. One of the authors raises the issue whether individuals could qualify as controllers when they decide to use a BC for a certain transaction, whereby the individual would both be a data subject as a data controller, which would turn the conceptual framework of the GDPR on its head.[77] Other than what the author seems to think, this is not a new issue. Also, here we see that the internet (and social media networks in particular) already presented us with a similar '*conundrum*,' which has already been adequately solved within the EU data protection framework. The underlying issue was at the time (2008) well phrased by the International Working Group on Data Protection in Telecommunications:[78]

> With respect to privacy, one of the most fundamental challenges may be in the fact that most of the personal information published in social networks is being published at the initiative of the users and based on their consent. While 'traditional' privacy regulation is concerned with defining rules to protect citizens against processing of personal data by the public administration and businesses.

As data subjects themselves publish their personal data on social media, for example, the social media networks argued it was not responsible (i.e. did not qualify as the controller) for the processing of these personal data but rather the data subjects themselves. This posed the question whether EU data protection laws were also meant to protect data subjects against themselves. Clarity was brought by the Working Party 29[79] in its 2009 opinion on how to apply EU data protection law to social networks:[80]

> Social Network Service (SNS) providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the 'basic' services related to user management (e.g. registration and deletion of accounts) and SNS should ensure privacy-friendly and free of charge default settings.

Disruption, and the Case of Network Contracts', in L. DiMatteo, M. Cannarsa & C. Poncibo (eds), *Smart Contracts and Blockchain Technology: Role of Contract Law*, (Cambridge University Press 2019), Ch. 12 (forthcoming), pp 2-3, describing as a development the growing interest in 'co-opting new technologies (either alongside or in the place of rules) as regulatory instruments.'

77 M. Finck, *MPI Paper* (2017), p 17.

78 International Working Group on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Network Services – Rome Memorandum* (2008), https://www.gpdp.it/documents/10160/10704/1531476, p 1 (last visited 18 November 2018).

79 The predecessor of the European Data Protection Board under GDPR.

80 Art. 29 Data Protection Working Party, *Opinion 5/2009 on online social networking* (2009), http://collections.internetmemory.org/haeu/20171122154023/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf, p 5 (last visited 18 November 2018).

22. Applying this reasoning to the BC, it is the organization (whether alone or jointly with others) offering the BC that provides for the 'means for processing the user data'. It is this organization that therefore has the responsibility to ensure that these 'means' are developed based on privacy-by-design requirements. Stakeholders can therefore not just launch new technologies and then take not responsibilities for their use.[81] This is why it is unlikely that public BC with no governance mechanism whatsoever will be acceptable to regulators if these BCs are intended for large scale use by consumers.

4. So no Data Protection Issues at all?

23. The foregoing does not mean that there are no issues remaining. If we refer back to the issues raised by the authors (see section 2), my conclusion is that the issue of jurisdiction and enforcement will not materialize in practice. The other issues raised are due to the immutable and inherently transparent character of BC, which (to a certain extent) also applies for private/consortium BC and which may make it impossible to respond to rights of individuals to have their data corrected or deleted, as a result of which the right to be forgotten will also be impossible to enforce. Again, I want to put the issues first in a broader context.

4.1. Issues with BC are not Specific for Data Protection only

24. Both the inherent immutability and transparency of current BC are not just an issue from the perspective of data protection for individuals. For example, transparency is equally an issue for companies[82] and may be further contrary to confidential requirements applicable to financial institutions and health care professionals.[83] The immutability of the BC does further not sit well with (i)

81 C. Wirth & M. Kolain, 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data', *Reports of the European Society for Socially Embedded Technologies* (2018), dx.doi.org/10.18420/blockchain2018_03, p 5 (last visited 18 November 2018).

82 See on transparency: V. Buterin, 'Privacy on the Blockchain', *Ethereum Blog* (15 January 2016): 'As seductive as a blockchain's other advantages are, neither companies or individuals are particularly keen on publishing all of their information onto a public database that can be arbitrarily read without any restrictions by one's own government, foreign governments, family members, coworkers and business competitors.'

83 Digital Asset Platform, *Non-technical White Paper* (2016), bit.ly/2mmwje7, p 7: 'confidential data should never be stored by a party not entitled to view that information, even if obfuscated or encrypted. As such, any potential solution designed for financial institutions must physically segregate confidential data' (last visited 18 November 2018). See also R. Ribitzki et al., *Blockchain in Healthcare Today* (2018), p 3: 'in most healthcare blockchains, sensitive information will be stored on the blockchain and only authorized entities should be given access to this information, making private and permissioned blockchains more appropriate'.

smart contracts in more complex transactions (as contracts often have to be amended for unforeseen circumstances),[84] (ii) with technological malfunction (including in case of interference by hackers)[85] and (iii) more in general with human messiness (known to lose their BC private key).[86] Solving these issues will require solving the immutability of the BC, which may well also solve the issue of being able to respond to requests for deletion and the right to be forgotten.

25. And lastly, storing too many data (especially transaction data) on the BC takes currently still too much energy both to run and cool the machines[87] which hampers the efficiency of the BC from an operational perspective. Suggestions to address this are to save block space by separating (segregating) the signature ('witness') information from the transaction data (the 'payload') so the network can increase the transactions processed.[88] These measures may well also to a certain extent mitigate transparency issues.

4.2. The Right To Deletion is not Absolute

26. The fact that the immutability issue is not addressed does not automatically mean that BC is therefore not suitable for all applications. Illustrative here is the

---

84 T. Tjong Tjin Tai, 'Formalizing contract law for smart contracts', *ICAIL* (2017), www.cs.bath.ac.uk/smartlaw2017/papers/SmartLaw2017_paper_1.pdf, https://ssrn.com/abstract=3038800, p 4: 'The immutability means that contracts cannot keep up with changing circumstances' (last visited 18 November 2018); and T. Tjong Tjin Tai, in his contribution to *ERLP*: 'Force Majeure and Excuses in Smart Contracts': 'smart contracts are not very well suited to deal with the finesses that are currently expected when it comes to excuses to performance'.

85 L. DiMatteo & C. Poncibo, in their contribution to *ERLP*, 'Quandary of smart contracts and remedies: The role of contract law and self-help remedies', describe the Ethereum incident, whereby hackers managed to steal 3.6 million of the cryptocurrency Ether (with a total value of about 50 million USD), which led the Ethereum community to agree to a hard-fork spitting up the BC (which shows that immutability of the BC is not never a given). See for different forms of malfunctioning: B. Brownsword, Ch. 12, 'Smart Transactional Technologies, Legal Disruption, and the Case of Network Contracts', L. DiMatteo, M. Cannarsa & C. Poncibo (eds), *Smart Contracts and Blockchain Technology: Role of Contract Law*, (Cambridge University Press 2019) (forthcoming).

86 The issue of human messiness is well described in more general terms by D. Tapscott & A. Tapscott, *Blockchain Revolution, How the Technology Behind BITCOIN and Other CRYPTOCURRENCIES is Changing the World* (Penguin 2016), p 24: 'Today, many people count on their bank or credit-card company, even talking with a real person, when they make an accounting error, forget their passwords, or lose their wallets or chequebooks. Most people with bank accounts in developed economies aren't in the habit of backing up their money on a flash drive or a second device, securing their passwords so they needn't rely on a service provider's password reset function, or keeping these backups in separate locations so that, if they lose their computer and all other possessions in a house fire, they don't lose their money.'

87 Tapscott & Tapscott, 'Realizing the Potential of Blockchain', p 14.

88 See on the 'segregated witness' (SegWit) solution proposed for the bitcoin protocol: Tapscott & Tapscott, 'Realizing the Potential of Blockchain', p 11.

judgment of the European Court of Justice in the *Manni* case.[89] The plaintiff (Mr Manni) requested deletion of his personal information from the Italian public company register where information on his prior bankruptcy was recorded. He argued that this record in the company register was widely reused by data brokers, as a result whereof his reputation was prejudiced having a detrimental effect on his new business. The ECJ balanced the public interest in the legal certainty in trade and transparency of business information in the company register with the fundamental right to data protection and concluded that, in this case, the interference with the rights to data protection was not disproportionate taking into account the limited amount of personal information held in the company register.

27. In line with the above ruling, registering limited personal data in a BC for public registers like land ownership, trademark ownership, company registers, etc., may therefore well be justified. The above case entails that a balancing of interests should be made for each BC application. For other use cases, the balancing test may well conclude that, for certain use cases, BC will not be suitable as the impact on data protection will be disproportionate compared to the interest served with using the BC. An example of the latter would be if BC would be applied to provide air passengers with expedited access through the airport, meanwhile also recording all money spent in shops and restaurants at airports, subsequent transport and accommodations on the BC for purposes of a loyalty program.[90] It will not require much imagination that also using BC for the commercial loyalty program would be disproportionate.[91]

4.3. Privacy-by-Design Options

28. The immutability and transparency issues associated with both public and private/consortium BC can, to a large extent, be addressed by implementing privacy-by-design measures.

In its most basic form, a BC can be used to store plain text information or encrypted text on the ledger, which information can be accessed by those who have *read* rights. Naturally, this is not desirable from a privacy perspective but also not desirable from an economic perspective. Storing all information on the BC takes up a large amount of space on the BC. This means that fewer transactions can be processed per block on the chain and that a large amount of storage capacity is required. Therefore, most BC applications store part of the transaction in hashed form to prevent that everyone can access the information and to increase the

89 ECJ (9 March 2017), *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, ECLI:EU:C:2017:197.

90 See for a loyalty program based on BC: 'Loyal Web Page', https//loyyal.com/ (last visited 18 November 2018).

91 Knowing that any such data relating to travel of individuals through airports will be prone to law enforcement access requests.

number of transactions that can be stored on a single block. For example, basic BC applications store a plain text header on the block (block header)[92] and a hashed part that includes the payload[93] of the transaction.[94]

29. The following privacy-by-design solutions can be used to create a more privacy-friendly BC application than the example described above that consists of a plain text header and a hashed payload:

- **Limit ledger storage.** The original Bitcoin BC store all transactions since the start of the chain (i.e. dating back to the 'genesis block'), on every node. This makes it almost impossible to make changes to prior blocks and thus provides for an indisputable ledger for all prior transactions. The creator of the new block provides a unique hash of the information to each of the nodes. The nodes have access to the information included on the new block and each re-do the mathematical computation done by the creator of a block. If the result is the same hashed value, the block is verified and can be added to the BC. By storing all blocks of the chain (i.e. the full ledger) on every node, it is almost impossible to make changes to prior blocks. In this manner an indisputable ledger is provided for all prior transactions. However, this also means that the personal data included on the ledger are shared with a large number of nodes (Bitcoin has approximately 9.500 nodes). Storing so many instances of personal data is at odds with the data minimization and confidentiality principles of the GDPR, which requires access to personal data to be limited to the fewest possible recipients.

  A privacy-by-design solution would be to store the entire ledger on one (or a few) instances only, and to instruct all other nodes to delete the information on a new block after verification has taken place. This will still enable the nodes to fulfil their verification function, while at the same time the full ledger can still be consulted if so required for verification purposes. This change in design will not only limit the storage of personal data and increase confidentiality, but also has economic advantages, such as saving storage capacity and energy consumption.

92 The block header contains metadata about the block, such as the version of the BC, an identification number of the previous block on the chain and information on the creator of the block.

93 The payload of a block contains the actual transactions (or other information for which the BC is used) included in a block.

94 M. Finck, *MPI Paper* (2017), p 5.

- **Zero-knowledge proof.** Another privacy-by-design solution for the current practice of storing all blocks of the chain on each node, is the concept of non-interactive zero-knowledge proof. This solution makes it possible for nodes to verify the correctness of the hash provided by the creator of the block, without having to re-do the mathematical computation done by the creator of a block or even learning what was executed. For example, the proposed currency Zerocoin[95] works as follows. When a coin is purchased, a serial number is attributed to the coin, which can only be revealed using a random number. Using these two numbers, a user can generate a zero-knowledge proof for the fact that the user knows both the serial number and the random number. This zero-knowledge proof can then be verified by the network without having access to the coin's serial number or the random number.[96]

  The potential use of zero-knowledge proof is not limited to the transfer of coins using BC, but can also be used to verify any computation without having access to the underlying information. This enables nodes to reach consensus on a new block, without accessing the information on that block, and thus without sharing the personal data included on that block with the nodes.

- **Pruning.** As set out above, most BC applications store all blocks infinitely. Storing data infinitely is, by definition, at odds with the GDPR's data minimization and storage limitation principles, but also requires ever-increasing storage capacity. For example, during a stress test, the size of the BC of an Ethereum client increased to 40 gigabytes in the first three months of the test.[97]

  A privacy-by-design solution to infinite storage is pruning. Pruning enables the node to verify a new block without having to process all historical transactions. Instead the nodes download as much block-headers as they can and determine which header is on the end of the longest chain. Starting from this header on the longest chain, the node goes back 100 blocks to verify that the chain matches up. Because this verification process removes the need for retaining the entire chain history for verification purposes, this allows for the

95 I. Miers, C. Garman, M. Greend & A.D. Rubin, 'Zerocoin: Anonymous Distributed E-Cash from Bitcoin' (2013), *IEEE*, https://ieeexplore.ieee.org/document/6547123 (last visited 18 November 2018).

96 Miers et al., 'Zerocoin', p 398.

97 V. Buterin, 'State Tree Pruning' *Ethereum Blog* (2015), https://blog.ethereum.org/2015/06/26/state-tree-pruning/ **(Last visited 18 November 2018).**

removal of unused blocks, implementing data minimization into the BC as well as drastically lowering required storage capacity.[98] To ensure that no data is lost, the unused blocks can be stored in one or more archive nodes, which store all data just in case the rest of the network needs them in the future, but the 'active' nodes no longer have to process these archived blocks.

- **Editable BC.** A radical approach that solves the immutability of BC is the editable BC, for which Accenture has been awarded a patent.[99] The editable BC uses the 'chameleon' hash function, which allows for changing the underlying information without changing the outcome of the hash function. This allows for changes to the underlying information of which the hash is already included on the BC, which makes it possible to correct (human) error or intentional (fraudulent) inaccuracies on the BC. This would allow for the execution of individuals' rights under the GDPR, e.g. to correction and to be forgotten.

  Solving the immutability of BC comes at a price. To a large extent, the trust in BC application relies on the network's consensus on the content of a block and the immutability of the content thereafter. When removing this immutability, other measures should be implemented to retain (or gain) sufficient trust in the BC application for individuals and organizations to use it as a record of their transactions. The trust in a BC application could be retained if, for example, only a single trusted entity can make changes, similar to the fact that only governments can make certain changes to governmental public registries. A different solution could be to implement a very strict change management procedure, which could include a consensus mechanism that verifies the legitimacy of a change. In any event, changes will have to be strictly logged to ensure that changes can always be reviewed and explained in the future.

---

98 *See* V. Buterin, 'State Tree Pruning' *Ethereum Blog* (2015), where the author explains that a BC can be pruned by tracking when a (part of) a block drops from the Merkle tree, which happens if it is no longer being used. These (parts of) blocks can be stored on 'death row', from which it can be retrieved if it would be used shortly after being dropped from the Merkle tree. The duration of the 'death row' can be determined by the BC provider; the longer this period, the less the archive node will have to be used, but the more storage space will be required for the active nodes to process a new block.

99 ACCENTURE 'Editing the Uneditable Blockchain, Why distributed ledger technology must adapt to an imperfect world' (2016), newsroom.accenture.com/content/1101/files/Cross-FSBC.pdf (last visited 18 November 2018).

- **BC identity management.** A final, even more radical privacy-by-design solution is not to store personal data (whether in hashed form or otherwise) on-chain at all. Rather, the BC could be used for 'self-sovereign' identity management.

  In the offline world, an individual's identity is mostly established by verifying an individual's driver's license or passport. The strength of this system follows from a trusted central governmental authority that provides these proofs of identity. As the online world does not follow the national boundaries of the offline world, it is difficult to appoint such trusted centralized authority for an online proof of identity.[100] By now, there are many initiatives to provide individuals with a digital identity.[101] An example of how BC can be deployed for online identify management is the initiative of Microsoft and Accenture providing a BC based solution designed to allow individuals with direct control over who has access to their personal data. Rather than that all service providers each collect and store the personal data required for providing services to an individual, the personal data are stored off-chain and the system only calls on these data when the individual grants access, whereby access can be limited both in scope and in time.[102] For example, when an individual needs to prove his or her identity when renting a car, the access to the identifying information can be limited to what is necessary to provide this proof and for a short period of time only.

  Decentralized identity management has a number of benefits. From a privacy point of view, it enables individuals to take back control over their digital identity, coined the 'self-sovereign identity'.[103] Currently, many individuals are, for example, not

100 See for an overview of identity management issues and publications relating to BC: the BLOCKCHAIN HUB, 'Identity as a Bottleneck for Blockchain, The Road to Self Sovereign Identity' (October 2017), blockchainhub.net/blog/blog/decentralized-identity-blockchain/ (last visited 18 November 2018); J. Eberhardt & S. Tai, 'On or Off the Blockchain? Insights on Off-Chaining Computation and Data, Information Systems Engineering (ISE)', *TU Berlin, Germany* (2017), fje,stg@ise.tu-berlin.de, at http://www.ise.tu-berlin.de/filead min/fg308/publications/2017/2017-eberhardt-tai-offchaining-patterns.pdf (last visited 18 November 2018); V. Buterin, *Ethereum Blog* (2016); P. de Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies', 9. *Journal of Peer Production 1*, CNRS – Berkman Center for Internet & Society at Harvard (2016).

101 S. Sater, *Tulane University* (2017), p 31.

102 Accenture, Microsoft Create Blockchain Solution to Support ID2020, *Accenture Newsroom* (June 2017), https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm (last visited 18 November 2018).

103 A. Tobin & D. Reed, *SOVRIN FOUNDATION 1* (2016), p 3.

aware of the use of their digital identity and personal data for advertising purposes. By using a decentralized identity system, individuals would be able to decide who to give access to which information for which period of time. A single decentralized identity system also has economic benefits. Right now, a large number of companies are storing similar information about the same individuals. A decentralized identity management system makes this duplicated storage obsolete and ensures that companies have access to up-to-date information on an individual, insofar as the individual wants the company to have such access.

The use of BC for decentralized identity management is a clear example of the variety of uses of BC. The well-known use cases of BC are mostly focused on administering transactions, but BC can also be deployed for privacy enhancing purposes.

5. Conclusion

30. BC technology is still in its infancy and will require further development to overcome the shortcomings of the initial public (Bitcoin) BC, including implementation of privacy-by-design requirements under the GDPR. This is an expected life cycle of development of new technologies for new use cases and already new BC applications show promising solutions and privacy-by-design features. The review of each of the potential data protection issues shows that these can likely be addressed to ensure compliance with the GDPR. The conclusion is that the GDPR is well able to regulate also this new technology. This does, however, not mean that BC will thus be suitable for all use and deployment cases or that no other governance issues remain. It is clear that BC is set to disrupt existing business models and that further thinking is required how best to regulate this new technology. Without many concrete deployment cases available yet, it is difficult to foretell all impacts on society and therefore how such regulation (if any) would exactly look like. The call from industry stakeholders for specific guidance on privacy-by-design requirements for BC is therefore too premature and may even hamper new developments.