CEJ
COMPLIANCE
ELLIANCE
JOURNAL

BLOCKCHAIN IN EU E-HEALTH – BLOCKED BY THE BARRIER OF DATA PROTECTION?

Ulrich M. Gassner

AUTHOR

Ulrich M. Gassner is a professor at the Law School of the University of Augsburg, Germany, and the founding director of the Center for E-Health Law. His main research interests include health law, pharmaceutical law, constitutional, and administrative law and data protection law. His publication list counts more than hundred books and articles related to health law. He also is co-editor of several law journals and book series. Furthermore, Ulrich M. Gassner advises private and public clients on a broad range of health law matters, with a focus on e-health law and pharmaceutical law.

ABSTRACT

Compliance with data protection requirements is always a tricky business and even more intricate when it comes to cutting-edge technologies such as distributed ledger technology (DLT), better known as Block Chain Technology (BCT). These difficulties increase even more when the personal data concerned is accorded a special level of protection, as is the case with health data. The following article aims to describe and analyze the legal issues associated with this scenario. The focus here is on the European Union's (EU) General Data Protection Regulation (GDPR)[1], which took effect on May 25, 2018. Furthermore, the functionality of BCT and its possible fields of application in healthcare will be outlined.

1 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) (OJ L 119 of 4.5.2016, p. 1).

TABLE OF CONTENTS

I. HYPE OR HOPE?

Block Chain Technology (BCT) has recently been referred to as "the most disruptive tech in decades".[2] Others consider it a fundamental technology that "has the potential to create new foundations for our economic and social systems."[3] In that respect, the Gartner Hype Cycle, introduced in 1995 by the technology analyst firm Gartner, Inc., proposes useful guidance. The hype cycle model traces the evolution of technological innovations in terms of expectations or visibility of the value of the technology. It explains the path that technologies generally take, from their initial introduction into the market until their eventual maturation into useful components of broader solutions.[4] According to this model, the five key phases of a technology's life cycle are:

(1) Innovation Trigger: A potential technology breakthrough kicks things off. Early proof-of-concept stories and media interest trigger significant publicity. Often no usable products exist and commercial viability is unproven.
(2) Peak of Inflated Expectations: Early publicity produces a number of success stories – often accompanied by scores of failures.
(3) Trough of Disillusionment: Interest wanes as experiments and implementations fail to deliver. Producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.
(4) Slope of Enlightenment: More instances of how the technology can benefit the enterprise start to crystallize and become more widely understood. Second- and third-generation products appear from technology providers. More enterprises fund pilots; conservative companies remain cautious.
(5) Plateau of Productivity: Mainstream adoption starts to take off. Criteria for assessing provider viability are more clearly defined. The technology's broad market applicability and relevance are clearly paying off.

In a recent study based on data from more than 3,100 CIOs from 98 countries Gartner sees BCT as a whole at the Peak of Inflated Expectations phase, whereas blockchain in e-health is still assigned to the phase of Innovation Trigger,[5] as most initiatives are still in alpha or beta stage. But without any doubt BCT in e-health will rapidly ascend to the

---

2 Lucas Mearian, *What is blockchain? The most disruptive tech in decades*, COMPUTERWORLD (May 31, 2018 1:35 PM PT), https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html?page=2 (last visited Aug. 20, 2018, 01:30 PM).

3 MARCO IANSITI & KARIM R. LAKHANI, THE TRUTH ABOUT BLOCKCHAIN, IN HBR'S 10 MUST READS 2018: THE DEFINITIVE MANAGEMENT IDEAS OF THE YEAR FROM HARVARD BUSINESS REVIEW 159 (2018).

4 See for a critical analysis, Martin Steinert & Ozgur Dedehayir, *The hype cycle model: A review and future directions*, 108 TECHNOL. FORECAST. SOC. CHANGE 28 ff. (July 2016).

5 GARTNER (ED.), BLOCKCHAIN STATUS 2018: MARKET ADOPTION REALITY (2018), quoted by: Christiane Pütter, *Erwartungen an Blockchain zurückstutzen*, CIO (June 22, 2018), https://www.cio.de/a/erwartungen-an-blockchain-zurueckstutzen,3580750 (last visited Aug. 20, 2018, 01:30 PM).

Peak of Inflated Expectations phase. Consequently, there is some evidence that the excitement around using BCT in healthcare is growing.[6] An example of this may be the somewhat evangelical fervor of some over-enthusiastic early adopters especially in the U.S., but also in other tech-savvy countries. Others argue that BCT in healthcare is all hype – a technological hammer looking for a nail – and that the complexities of health information could prevent its practical use.[7] However, most people seem to have recognized that, when the dust of the hype clears, BCT may have a significant role to play as a main component of the digital transformation of the healthcare sector. According to the Gartner study, this technology is upwards of only ten years from mainstream adoption. Therefore, it comes as no surprise that many advocates are already pointing to BCT's potential to revolutionize healthcare in terms of the secure and efficient sharing of health data, of fostering patient empowerment, etc.[8]

Even good old Europe has jumped on the bandwagon. Within the framework of EU's Horizon 2020 research and innovation program, the research project My Health My Data (MHMD) has been funded 3,455.190 EUR (ca. 4 mio. USD). It aims to use BCT to enable medical data to be stored and transmitted safely and effectively. The MHMD project is centered on the connection between organizations and individuals, encouraging hospitals to start making anonymized data available for open research, while prompting citizens to become the ultimate owners and controllers of their health data. For these purposes, it will create a platform relying on BCT.[9]

---

6 See, e.g., William Gordon, Adam Wright & Adam Landman, *Blockchain in Health Care: Decoding the Hype*, NEJM Catalyst (February 9, 2017), https://catalyst.nejm.org/decoding-blockchain-technology-health/ (last visited Sept. 17, 2018, 10:05 AM).

7 Id.

8 See, e.g., CHRISTINA CZESCHIK & RATKO STAMBOLIJA, A QUICK GUIDE TO BLOCKCHAIN IN HEALTHCARE, 18 et seq. and passim (2nd ed. 2018); PETER B. NICHOL, THE POWER OF BLOCKCHAIN FOR HEALTHCARE: HOW BLOCKCHAIN WILL IGNITE THE FUTURE OF HEALTHCARE, 14 et seq. (2017); AXEL SCHUMACHER, BLOCKCHAIN & HEALTHCARE STRATEGY GUIDE 2017: REINVENTING HEALTHCARE: TOWARDS A GLOBAL, BLOCKCHAIN-BASED PRECISION MEDICINE, 2 et seq. (2017); Devon S. Connor-Green, *Blockchain in Heathcare Data*, 21 INTELL. PROP. & TECH. L. J. 93, at 106-07 (2017); Leslie Mertz, *(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution*, 9(3) IEEE PULSe 4 (2018); Juan M. Roman-Belmonte, *Hortensia De la Corte-Rodriguez & E. Carlos Rodriguez-Merchan, How blockchain technology can change medicine*, 130 POSTGRAD MED 420 (2018); Gordon, Wright & Landman, supra note 5; David Randall, Pradeep Goel & Ramzi Abujamra, *Blockchain Applications and Use Cases in Health Information Technology*, 8 J HEALTH MED INFORMAT 276 (2017); Stanislaw P. Stawicki, Michael S. Firstenberg & Thomas J. Papadimos, *What's new in academic medicine? Blockchain technology in health-care: Bigger, better, fairer, faster, and leaner*, 4(1) INT J ACAD MED 1 (2018); Viola Hoffmann, *Blockchain technology as an opportunity for more transparency and self-determination*, GESUNDHEITSINDUSTRIE BW (January 15, 2018), https://www.gesundheitsindustrie-bw.de/en/article/news/blockchain-technology-as-an-opportunity-for-more-transparency-and-self-determination/ (last visited Sept. 17, 2018, 10:40 AM).

9 My health, my data - A New Paradigm in Healthcare Data Privacy and Security, (last visited Oct. 10, 2018, 10:40 AM) http://www.myhealthmydata.eu/.

II. HOW DOES BCT WORK?

BCT was the brainchild of the Bitcoin creator(s) acting under the pseudonym Satoshi Nakamoto. Bitcoin saw the light of day in a paper of 2008 and was conceptualized as a decentralized, cryptographically empowered currency framework for financial interactions without an intermediary. However, while cryptocurrencies are part of the blockchain phenomena, BCT is not limited to cryptocurrencies. Rather, BCT has the potential to restructure economic and social systems and even create new foundations in them. So far there have also been use cases for personal identity verification, land-title deeds, intellectual property ownerships, public and financial records, and digital (or "smart") contracts that automatically execute when certain pre-defined conditions are met. From a technological point of view a smart contract means a piece of software that controls and/or documents or even effects a legally relevant activity.
In general, the blockchain may be defined as a public (distributed) ledger which works like a log by keeping a growing list of records, called "blocks", of all transactions in a chronological order, secured by an appropriate consensus mechanism and providing a record that is, at least in principle,[10] immutable. BCT is also often considered as a decentralized database using the peer-to-peer principle. As opposed to a traditional (e.g., relational) database, there is no central ownership. Instead, information is managed through the consensus of the network members, who cooperate to decide what gets added to the database. In sum, the exceptional characteristics of BCT include immutability, irreversibility, decentralization, persistence and anonymity.[11]

The three main components of BCT are:

(1) A peer-to-peer computer network,
(2) a network protocol, and
(3) a consensus mechanism.[12]

Basically, the peer-to-peer network can be public (unpermissioned, open) or private (permissioned[13], closed). The main differences between these two types are as follows:

---

10 Cf., e.g., Gideon Greenspan, *The Blockchain Immutability Myth*, MULTICHAIN (May 4, 2017), https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/ (last visited Sept. 17, 2018, 10:40 AM).

11 Cf., e.g., Dylan Yaga, Peter Mell, Nik Roby & Karen Scarfone, *Draft Nistir 8202: Blockchain Technology Overview*, NIST (January 2018), https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf (last visited Sept. 17, 2018, 10:40 AM); ARSHDEEP BAHGA & VIJAY MADISETTI, BLOCKCHAIN APPLICATIONS. A HANDS-ON APPROACH, 20-23 (2017); Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, & Gautam Das, *Everything you Wanted to Know about the Blockchain*, 7(4) IEEE CONSUMER ELECTRONICS MAGAZINE 6 (2018).

12 CZESCHIK & STAMBOLIJA, supra note 8, at 10 et seq.

13 Furthermore, permissioned blockchains which allow anyone to join a network once identity and role are defined have to be differentiated from private blockchains, which allow only known or internal nodes to participate in the network.

(1) Control over the network. Public chains are controlled by the wide community of core developers, users, and miners or validators. In turn, private blockchains are governed out by a specific group of people or institutions.
(2) Consensus mechanism (see below).
(3) Application. While public chains are mostly used for payments (as seen in Bitcoin) or as a platform for decentralized applications' development (as seen in Ethereum), almost all private chains are used for solving specific business tasks.[14] Accordingly, most healthcare BCT projects are based on private blockchains.[15]

Each computer in a specific network is called a "node". If everything is running per protocol, each node should have a copy of the entire ledger, which is sort of a local database. This means if one node disconnects or goes down, no data is lost and the ledger's consistency will be kept.
The underlying principle of any transaction is that of public/private key encryption in order to generate digital signatures. A user has two keys: a public key to encrypt data and a private key to decrypt them. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash). And unless one of the parties to the transaction decides to link a public key to a known identity it is impossible to match transactions to individuals or organizations. Although anyone can see all the transactions on the blockchain no personal information is linked to them or made public. This allows any party to validate the integrity of the transaction ledger without violating the privacy of the parties involved in the transaction.
All transactions are verified by a consensus mechanism which is a set of rules utilized by the network to verify each transaction and confirm the current state of the blockchain. In most cases, public chains use Proof-of-Work (PoW) systems, in which so-called "miners" solve cryptographic puzzles to "mine" a block in order to add to the blockchain. This process requires an immense amount of energy and computational usage. When a miner solves the puzzle, they present their block to the network for verification. Verifying whether the block belongs to the chain or not is an extremely simple process. In contrast, private blockchains mostly use well-known and established consensus algorithms with authentified participants such as modified Proof-of-Authority (PoA). In PoA-based networks, transactions and blocks are validated by approved accounts, known as validators, who replace miners. However, as there is no "perfect" consensus mechanism, the search for a truly decentralized consensus mechanism is still going on.[16]
In sum, the result of BCT is an expansive and distributed source of truth built not from trust, but through cryptographically enforced consensus. As its most important attribute can be considered its immutability: once something has been added to the blockchain, it

14 See, e.g., Ivan Grekov, *Is the Right to Be Forgotten a Real Problem for Blockchain?*, LAWLESS.TECH (Apr. 16, 2018), https://lawless.tech/is-the-right-to-be-forgotten-a-real-problem-for-blockchain/ (last visited Sept. 17, 2018, 10:20 AM).

15 CZESCHIK & STAMBOLIJA, supra note 8, at 10.

16 CZESCHIK & STAMBOLIJA, supra note 8, at 11; see also, e.g., Basic Primer: Blockchain Consensus Protocol, Blockgeeks, https://blockgeeks.com/guides/blockchain-consensus/ (last visited Sept. 17, 2018, 10:20 AM).

is permanently stored in a large number of computers.[17]

III. HOW CAN BCT BE APPLIED TO HEALTHCARE?

Realized and probable applications of BCT in healthcare can be divided into eight main areas, namely electronic health records (EHR) management and interoperability, biomedical research, medication planning and management, revenue cycle management (RCM), procurement policies and supply chain management (SCM), internet of medical things (IoMT), health professions education, and international medicine and global health.

A. EHR management and interoperability

Most healthcare systems suffer from the siloing of patients' health data and a lack of interoperability between different domains. Several current health record systems – in the U.S., for example, as well as in most European countries with the exception of Estonia[18] – are composed of an enormous number of disconnected databases. Health records are usually spread across various institutions, health care providers, and suppliers that often use incompatible databases, without full access to a shared patient database. This lack of interoperability leads to enormous inefficiencies.[19]
BCT would provide the ability to replace these disparate systems with an integrated system that, with the use of smart contracts and fully auditable history, enables peer-to-peer interoperability among participants (such as physicians, medical institutions, insurance companies, and pharmacies) within transactions.[20] Using BCT as a data management tool would be especially useful for the implementation of so-called integrated healthcare models, in which the stationary and ambulatory sectors need to exchange information to create an efficient and agreeable patient journey.[21] Instant access to an agreed set of data about a patient would also mean better data for better care in acute, life-threatening situations

17 WRIGHT & LANDMAN, supra note 6.

18 This small EU member state was the first country to implement a blockchain into their electronic healthcare record (EHR) system with the collaboration of a local company named Guardtime, using keyless signature infrastructure (KSI), Danielle Siarri, The potential of blockchain in HER, Oct. 6, 2017, https://www.himss.eu/himss-blog/potential-blockchain-ehr [last visited Oct. 18, 2018, 10:40 AM]; Johnathon Marshall, *Estonia prescribes blockchain for healthcare data security*, PWC (March 16, 2017), http://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html (last visited Sept. 17, 2018, 10:10 AM); see also the official website https://e-estonia.com/blockchain-healthcare-estonian-experience/.

19 CZESCHIK & STAMBOLIJA, supra note 8, at 18.

20 Randall, Goel & Abujamra, supra note 8; Igor Radanović & Robert Likić; *Opportunities for Use of Blockchain Technology in Medicine*, APPL HEALTH ECON HEALTH POLICY (July 18, 2018), doi: 10.1007/s40258-018-0412-8; Arlindo Flavio da Conceição, Flavio Soares Correa da Silva, Vladimir Rocha, Angela Locoro & João Marcos Barguil, *Electronic Health Records using Blockchain Technology*, CORNELL UNIVERSITY LIBRARY (April 26, 2018, https://arxiv.org/abs/1804.10078 (last visited Sept. 17, 2018, 10:10 AM).

21 CZESCHIK & STAMBOLIJA, supra note 8, at 34.

and for better treatment of chronic longer-term conditions (e.g., diabetes[22]). Patients could be treated more quickly and in a more targeted way. As a result, for example, the duplication of examinations or treatments would be prevented, ultimately increasing efficiency.[23] Furthermore, sharing the ledger among the participants would bring transparency to the whole process of treatment, from monitoring drug compliance to facilitating cost controls.[24] In addition to offering interoperability, blockchain transactions would also have the advantage of being cryptographical and irrevocable, thus ensuring privacy across parties[25] and reducing fraud.[26] Moreover, in the BCT environment, the patient (or his relatives) would be able to designate by whom the data can be accessed (and at what level of access) by the use of keys that only users would be able to dispose of (either private or public).
The key management and the access control could be encoded in a chaincode, thus ensuring patients' autonomy and self-determination.[27]

B. Biomedical research

Lack of reproducibility, related to a wide range of scientific misconduct aspects, from errors to frauds, compromises the outcomes of clinical studies and undermines research quality. BCT offers the chance to tackle this huge medical challenge for contemporary biomedical research. Study data would be time stamped and publicly more transparent than now. All plans, consents, protocols, and outcomes could be stored in a blockchain. Furthermore, smart contracts could be used to link together several phases of a clinical study.[28] Additionally, as a more general factor, the application of BCT could bring about the access to a large pool of anonymous and encrypted medical data that could be used for personalized drug development and epidemiological studies.[29]

---

22 Simon Lebech Cichosz, Mads Nibe Stausholm, Thomas Kronborg, Peter Vestergaard & Ole Hejlesen, *How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept*, J DIABETES SCI TECHNOL (July 26, 2018), doi: 10.1177/1932296818790281.

23 Hoffmann, supra note 8.

24 Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher & Fusheng Wang, *How Blockchain Could Empower eHealth: An Application for Radiation Oncology, in:* Data Management and Analytics for Medicine and Healthcare 3, 4-5 (Edmon Begoli, Fusheng Wang & Gang Luo eds. 2017).

25 CZESCHIK & STAMBOLIJA, supra note 8, at 35; Randall, Goel & Abujamra, supra note 8.

26 Randall, Goel & Abujamra, supra note 8.

27 CZESCHIK & STAMBOLIJA, supra note 8, at 35-36; Dubovitskaya, Xu, Ryu, Schumacher & Wang, supra note 24, at 5; Radanović & Likić, supra note 20; Randall, Goel & Abujamra, supra note 8; Hoffmann, supra note 8.

28 Mehdi Benchoufi & Philippe Ravaud, *Blockchain technology for improving clinical research quality*, 18 TRIALS 335 (2017); Dubovitskaya, Xu, Ryu, Schumacher & Wang, supra note 24, at 5; Radanović & Likić, supra note 20.

29 Radanović & Likić, supra note 20.

C. Medication planning and management

Without any doubt, medication reconciliation is one of the most important tasks related to quality of care and patient safety. Using appropriate patient safety algorithms via BCT, medication errors, contraindications, and medication prescriptions could be reconciled near-instantaneously - without the need for time-consuming medication reconciliation processes.[30]

D. Revenue cycle management (RCM)

BCT can help hospitals and health systems to improve the performance of revenue cycle management by reducing denials and boosting patient collections because it allows payers, providers, and financial institutions to share information via private distributed ledgers.[31]

E. Procurement policies and supply chain management (SCM)

BCT could considerably improve procurement policies since it would ensure that the supply of goods is transparent, verifiable, and more efficient. Suppliers could be more easily controlled and, if necessary, held accountable for the quality of their products. The logistics of pharmaceutical and medical device manufacturers could profit from BCT especially as there is a high risk of substandard or counterfeited products entering the supply chain. By introducing smart contracts, checks and transactions could be carried out automatically. In transactions, in which no conflicts are detected, even payments might be automatized.[32]

F. Internet of medical things (IoMT)

IoMT refers to the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. Medical devices equipped with WiFi, Bluetooth, or other interfaces allow the machine-to-machine communication that is the basis of IoMT. The cybersecurity of the connected medical devices and the vulnerable sensitive data that passes through the IoMT could be ensured by BCT.[33]

---

30 CZESCHIK & STAMBOLIJA, supra note 8, at 20 et seq.; Stawicki, Firstenberg & Papadimos, supra note 8.

31 Kelly Gooch, *4 ways to improve RCM with blockchain*, Becker's Hospital CFO Report (March 28, 2018), https://www.beckershospitalreview.com/finance/4-ways-to-improve-rcm-with-blockchain.html (last visited Sept. 17, 2018, 10:10 AM).

32 CZESCHIK & STAMBOLIJA, supra note 8, at 23; Stawicki, Firstenberg & Papadimos, supra note 8.

33 CZESCHIK & STAMBOLIJA, supra note 8, at 23-4; Bernard Marr, *Blockchain And The Internet Of Things: 4 Important Benefits Of Combining These*, Forbes (Jan 28, 2018, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2018/01/28/blockchain-and-the-internet-of-things-4-important-benefits-of-combining-these-two-mega-trends/#50249c9a19e7 (last visited Sept. 17, 2018, 10:10 AM); Matthew Warner, Two Mega Trends Blockchain Technology to Secure Internet of Medical Things, Chain-Finance (Aug. 15, 2017, 1:35 AM),

G. Health professions education

Novel methods of health professions education have often been criticized for their lack of the ability to ascertain the origin, validity, and accountability of the knowledge that is created, shared, and acquired. If based on BCT it will potentially allow improved tracking of content and the individuals who create it, quantify educational impact on multiple generations of learners, and build a relative value of educational interventions.[34] Additionally, records on this digital ledger could continue to grow during the professional life of the physician, archiving attended conferences, written articles, and rates of successful treatments.[35]

H. International medicine and global health

In the area of academic international medicine and global health, blockchain-enabled assessment systems could lead to an alignment of effort allocation between settings (e.g. national and international), the immediate provision of much-needed assistance to low-resource environments, and the reduction of brain-drain that plagues areas in greatest need for healthcare delivery. In terms of its potential impact on the current global healthcare system, BCT could be one of the key components of ensuring both stability and sustainability in the future.[36]

IV. BCT VS. DATA PROTECTION?

A. Patient empowerment by BCT and privacy rules?

As of now, health information is widely controlled by insurance companies and funds, hospitals, doctors, and other intermediaries who, while claiming trustworthiness, are in a position to exploit that trust within essentially asymmetric power structures. BCT could reduce the role of these intermediaries, thus shifting the power balance in favor of the patients. It is capable of putting patients at the center of their health data and enabling data transactions not only to be secure, but also accessible and under the control of the individual patient. If implementing BCT can successfully re-distribute the control of health data back to individuals this could make individual access rights obsolete.[37]

---

http://www.chain-finance.com/2017/08/15/blockchain-technology-to-secure-internet-of-medical-things/ (last visited Sept. 17, 2018, 10:10 AM).

34 Eric Funk, Jeff Riddell, Felix Ankel & Daniel Cabrera, *Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education*, Acad Med. (June 12, 2018), doi: 10.1097/ACM.0000000000002326; Radanović & Likić, supra note 20.

35 Radanović & Likić, supra note 20.

36 Stawicki, Firstenberg & Papadimos, supra note 8.

37 Cf. Connor-Green, supra note 8, at 99, 106-07, referring to the U.S. legal situation.

However, BCT cannot solve all trust and privacy concerns surrounding health data protection. Therefore, it has been proposed that the U.S. federal regulation governing healthcare data privacy, the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[38] should be supplemented with stricter rules in line with the model of the GDPR[39]. Coupled with BCT, it would affirm a paradigm shift in the US-American legal landscape in terms of data ownership.[40] The GDPR, however, does not explicitly refer to the intrinsically problematic concept of personal data ownership. Rather, it follows merely from the wording of sentence 2 of its Recital[41] 7, "Natural persons should have control of their own personal data", that data subjects should be in control of their personal data.

The regulation paints the term "personal data" with a very broad stroke. It is defined in Article 4(1) GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person". It is well established that personal data that has been encrypted or hashed still qualifies as personal data within this definition as it is merely pseudonymized and not irreversibly anonymized.[42] It follows that not only personal data but also public keys used in BCT qualify as personal data, just like data relating to a natural person that is hashed to the chain.[43] As a consequence, cryptographically modified health data stored, e.g., on a distributed ledger of an integrated EHR, in addition to public keys, are subject to the GDPR.

Furthermore, as opposed to the narrower approach of the HIPAA Privacy Rule[44] all individuals, organizations, and companies that are either "controllers"[45] or "processors"[46]

---

38 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

39 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) (OJ L 119 of 4.5.2016, p. 1).

40 Connor-Green, supra note 8, at 99.

41 Recitals are important because they are used by the Court of Justice of the European Union (CJEU) and other EU institutions in order to interpret any Directive or Regulation.

42 MICHÈLE FINCK, BLOCKCHAINS AND DATA PROTECTION IN THE EUROPEAN UNION 10-11, SSRN (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322 (last visited Sept. 17, 2018, 4:20 PM); cf. further Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN, 20; but see BLOCKCHAIN BUNDESVERBAND, BLOCKCHAIN, DATA PROTECTION, AND THE GDPR 4 (2018).

43 FINCK, supra note 42, at 12-14.

44 See, e.g., Connor-Green, supra note 8, at 104-05.

45 A "data controller" is a party that determines the purposes and means of the processing of personal data, see Article 4(7) of the GDPR.

46 A "data processor" is a party that processes personal data on behalf of the controller, see Article 4(8) of the GDPR.

of personal data are covered by the GDPR. This does not mean that the regulation applies to all processing of personal data of EU citizens or residents, as often incorrectly stated. Rather, pursuant to Recital 80 of the GDPR, its territorial scope includes the processing of personal data of someone "in the Union" by data controllers or processors outside, "where the processing activities are related to the offering of goods or services" to that person, even if they do not require payment. According to Recital 23 of the GDPR, the appropriate test is based on whether the organization "envisages" offering goods and services, not on whether it does in fact offer, supply, or simply obtain personal data.[47]
The goal of effective control by data subjects is accomplished by, inter alia, requiring explicit and informed consent for the collection and use of data (Articles 6(1)(1)(a) and 7 GDPR) and imposing stiff fines on data controllers or processors for non-compliance (Article 83 of the GDPR). One of the cores of the regulation is formed by eight fundamental and dispositive rights of the data subjects that are outlined below.

(1) The right to be informed (Articles 13 and14 of the GDPR): A data subject has the right to know how his or her data will be collected, processed, and stored, and for what purposes.
(2) The right to access information (Article 15 of the GDPR): A data subject has the right to know how his or her data has been collected, processed, and stored, what data exists, and for what purposes.
(3) The right to rectification (Article 16 of the GDPR): A data subject has the right to have inaccurate or incomplete data corrected.
(4) The right to erasure ("the right to be forgotten") (Articles 17 and 19 of the GDPR): A data subject has the right to have personal data permanently deleted without the need for a specific reason as to why he or she wishes to discontinue the data storage.
(5) The right to restriction of processing (Article 18 of the GDPR): A data subject has the right to block or suppress his or her personal data being processed or used.
(6) The right to data portability (Article 20 of the GDPR): A data subject has the right to transfer personal data from one data controller to another in a safe and secure way and in a commonly used and machine-readable format.
(7) The right to object to processing of personal data (Article 21 of the GDPR): A data subject has the right to object to being subject to public authorities or companies processing their data without explicit consent and to stop his or her personal data from being included in direct marketing databases.
(8) The right to not be subject to automated decision-making (Article 22 of the GDPR): A data subject has the right to demand human intervention, rather than having important decisions made solely by algorithm.

So, at first sight, there may be a case for supplementing the HIPAA by selected features

47 See, e.g., Pascal Schumacher, *Territorial cope of application of the GDPR – Change from the principle of territoriality to effects doctrine*, *in* New European General Data Protection Regulation. A Practitioner's Guide 38-39 (Daniel Rücker & Tobias Kugler eds., 2018); PAUL VOIGT & AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR), 26-29 (2017).

of the GDPR in order to improve health data privacy. But when looking at some of the data subject's rights mentioned above, the question may arise whether a decision has to be made between using BCT and applying GDPR-standards. For example, the right of erasure appears to be particularly at odds with the immutable nature that is at the core of BCT.[48] Consequently, the issue whether BCT and GDPR can co-exist, is to be examined in more detail below.

B. Does the GDPR block BCT?

1. Systemic tension

Arguably, BCT and the GDPR are profoundly incompatible even at a conceptual level as the data protection mechanisms developed for centralized data silos cannot be easily reconciled with a decentralized method of data storage and protection. However, personal data in a blockchain system that is encrypted or hashed is still subject to the GDPR and public keys used in BCT surroundings are qualified as personal data under EU law.[49] Herefrom results not only a risk that the GDPR renders the operation of blockchains unlawful. Rather, this tension reveals also a clash between the goals of the protection of privacy on the one hand, and the promotion of innovative technology on the other hand.[50] However, due to the different construction of unpermissioned and permissioned blockchains, the latter being dominant in healthcare, it is obvious that the latter cause minor difficulties from the point of view of data protection. In addition, technical solutions that can contribute to BCT's data protection compliance are feasible or have already been implemented. This is often overlooked in the sometimes quite simplistic public discussion.[51] We will turn to these issues below.

2. Personal data

While BCT allows for personal data to be stored in the same way as in a database, personal can also be stored "off chain" in a separate database and only linked to the blockchain via private and public cryptographic keys. Consequently, GDPR compliance can be ensured

---

48 See, e.g., Samuel Martinet, *GDPR and Blockchain: Is the New EU Data Protection Regulation a Threat or an Incentive?*, Cointelegraph (May 27, 2018), https://cointelegraph.com/news/gdpr-and-blockchain-is-the-new-eu-data-protection-regulation-a-threat-or-an-incentive (last visited Sept. 17, 2018, 10:10 AM).

49 See supra section IV.

50 Cf. FINCK, supra note 42, at 1-2, 28-29; cf. also Anne Toth, *Will GDPR block Blockchain?*, World Economic Forum (May 24, 2018), https://www.weforum.org/agenda/2018/05/will-gdpr-block-blockchain/ (last visited Sept. 17, 2018, 10:10 AM).

51 See, e.g., Gyula Pal, *The GDPR blockchain blind-spot: Regulating data and everything else*, IBM (Jun 26, 2018), https://www.ibm.com/blogs/blockchain/2018/06/the-gdpr-blockchain-blind-spot-regulating-data-and-everything-else/ (last visited Sept. 18, 2018, 01:15 AM); Toth, supra note 50

in that respect.[52] This would be the case, for example, if the EHR themselves continue to be stored in hospital databases, i.e., off the chain. However, such a workaround has the disadvantage that the benefits of transparency and data control with BCT are reduced. Thus, paradoxically, in this context the application of the GDPR leads to a result that is at odds is with its explicit goal that "natural persons should have control of their own personal data" (Recital 7).[53]
Unlike transactional data, public keys cannot be moved off-chain as they are quintessential components of the BCT. Different promising work-arounds have been developed recently, but it is difficult to say at this stage whether any of these techniques will be considered capable of anonymizing public keys for GDPR purposes.[54]

3. Legal status of participants

As the GDPR was designed in a pre-BCT-world with a clear division of responsibilities between controllers and processors, the legal status of the different participants in blockchain networks is rather ambiguous. Especially public blockchains do not fit cleanly in this model. Namely, nodes cannot be considered data controllers in such a setting as they do not determine the means and purposes of the processing of personal data sent to the network by a third party.[55] When it comes to private blockchains, however, it might still be possible to identify a central intermediary. A governance body may be established to oversee the permissioned network. This governance body could not only function as a data processor if it has influence over the purpose and means of processing within the meaning of Article 4(7) of the GDPR but also as a data controller who collects personal data from individuals serving as a single point of legal contact with the network.[56]

4. Data minimization

An important principle in the GDPR is data minimization. Article 5(1)(c) of the GDPR requires that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This principle is profoundly at

---

52 Cf. FINCK, supra note 42, at 11-12; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 4; Andries Van Humbeeck, The Blockchain-GDPR Paradox, TheLedger (Nov. 21, 2017), https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047 (last visited Sept. 18, 2018, 01:15 AM); Lucas Mearian, Will blockchain run afoul of GDPR? (Yes and no), Computerworld (May 7, 2018 3:02 AM PT), https://www.computerworld.com/article/3269750/blockchain/will-blockchain-run-afoul-of-gdpr-yes-and-no.html (last visited Sept. 17, 2018, 10:15 AM); Luke Sayer, *Comment: Can GDPR and blockchain co-exist?*, International Investment (May 4, 2018), http://www.internationalinvestment.net/comment/comment-can-gdpr-and-blockchain-co-exist/ (last visited Sept. 18, 2018, 01:15 AM).

53 Cf. Van Humbeeck, supra note 52.

54 FINCK, supra note 42, at 14-16.

55 FINCK, supra note 42, at 16-17; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 5-6.

56 FINCK, supra note 42, at 16; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 7.

odds with data storage in a blockchain since distributed ledgers are by definition ever-growing creatures accumulating further data with each additional block.[57]

5. The right to rectification

Data subjects' rights under Article 16 of the GDPR imply that a rectification request can be addressed to any or all nodes. Two technical hurdles arise in this context. First, even in a permissioned blockchain – standard in healthcare environments – the data subject will face difficulties to identify any or all of the owners of the nodes. Second, even if the data subject succeeds in submitting a claim under Article 16 GDPR, they are simply unable to change any of the encrypted data stored in blocks due to their immutable nature. Again, an off-chain solution may operate as a legal loophole in that respect.[58]

6. The right to access information

With respect to Article 15 of the GDPR similar practical difficulties arise. Controllers do not know what personal data is stored on the blockchains, since they normally handle only the encrypted or hashed version. Even if a data subject were successful in contacting the owner of a node, the latter would not be able to verify whether the personal data of a data subject has been processed. Off-chain storage can again facilitate GDPR compliance in relation to transactional data but not public keys.[59] This is all the more true when a governance body is established to oversee the permissioned network.

7. The right to erasure

According to Jan Philipp Albrecht, the former member of the European Parliament who shepherded the GDPR through the legislative process, the administratively easy exercise of the right to be forgotten "is where blockchain applications will run into problems and will probably not be GDPR compliant."[60] It is however common ground that the right to be forgotten cannot be straightforwardly applied to BCT, as immutability is one of the essential features of blockchains.[61] However, the insight has grown that there is no such thing as perfect immutability in blockchains. For instance, it is easy to undermine if all the participants in a chain decide to do so together.[62]

---

57 FINCK, supra note 42, at 20-21.

58 Cf. id. at 21-22.

59 Id. at 23 (relating to public blockchains).

60 Quoted in David Meyer, *Blockchain technology is on a collision course with EU privacy law*, The Privacy Advisor (Feb. 27, 2018), https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/ (last visited Sept. 17, 2018, 01:20 AM).

61 FINCK, supra note 42, at 23-24; Grekov, supra note 14.

62 Greenspan, supra note 10; see also Grekov, supra note 14.

Furthermore, the principle of immutability can be circumvented by an off-chain or similar solutions. Personal data which is recorded in a referenced encrypted and modifiable database as opposed to the blockchain itself, may be deleted in line with Article 17 of the GDPR.[63]
With respect to public keys, GDPR compliance is again more difficult to reach. Whether any of the several solutions that have been developed up to now can satisfy GDPR requirements remains to be seen.[64] Notwithstanding that, it seems to be worth mentioning that certain implementing acts of the EU member states have already directed themselves towards a softer version of the right to erasure. For instance, Section 35(1) of the German Federal Data Protection Act[65] provides that the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data if the "erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal".[66]

C. Does BCT support the GDPR

Despite the tension between technology and law outlined above, it comes not totally as a surprise that BCT is being increasingly considered as a mechanism to help control the use of personal data under the GDPR.[67] The reason is that both initiatives are aligned on the principles of secured and self-sovereign data.[68] A prominent example of this coincidence are the guiding principles of data protection by design and data protection by default. Article 25(1) of the GDPR requires data protection to be designed into the development of business processes for products and services. Specifically, the controller should have technical, procedural, and organizational measures - such as pseudonymization and encryption - in place in order to meet the requirements of the GDPR. Being based on advanced encryption technologies, BCT can support the implementation of GDPR-compliant solutions which also may be a reason for regulators and courts to look favorably at it.[69]

---

63 FINCK, supra note 42, at 24; CINDY COMPERT, MAURIZIO LUINETTI, & BERTRAND PORTIER , BLOCKCHAIN AND GDPR, IBM WHITE PAPER, 3, (2018), https://public.dhe.ibm.com/common/ssi/ecm/61/en/61014461usen/security-ibm-security-solutions-wg-white-paper-external-61014461usen-20180319.pdf (last visited Sept. 17, 2018, 01:20 AM).

64 FINCK, supra note 42, at 24; but see Grekov, supra note 14.

65 Federal Law Gazette I p. 2097.

66 Cf. FINCK, supra note 42, at 26; BLOCKCHAIN BUNDESVERBAND, supra note 42, at 8.

67 Cf., e.g., COMPERT, LUINETTI, & PORTIER, supra note 63; Mearian, supra note 52.

68 COMPERT, LUINETTI, & PORTIER, supra note 63, at 2.

69 FINCK, supra note 42, at 26, 30-31; COMPERT, LUINETTI, & PORTIER, supra note 63, at 6-7 (hinting at the example of the Estonian EHR system).

V. CONCLUSION AND OUTLOOK

In sum, BCT offers many benefits to patients, health care service providers, hospitals, medical researchers, caregivers, and other healthcare parties. It integrates the healthcare ecosystem by adding accountability and transparency, while preserving privacy and confidentiality.[70] This indicates at least partial concordance with the objectives of the GDPR. Thus, BCT can provide an alternative means of achieving the objectives of the GDPR.[71] Yet it is also equally true that there is a systemic tension between technology and privacy law. And without any doubt, some blockchains in healthcare, as currently designed,[72] are incompatible with the GDPR.

Considering that the GDPR was developed without taking BCT into account, it could at first glance be wise to amend it for blockchains.[73] Such a revision of the GDPR would acknowledge the fact that BCT creates order without law and implements private regulatory frameworks (lex cryptographia).[74] However, for the time being, there are hardly any signs of EU reform initiatives in that respect. The European Parliament's Committee on Industry, Research and Energy (ITRE) passed a resolution outlining the benefits of adopting DLT on May 16, 2018, without explicitly requiring amendments to the GDPR.[75] The ITRE only emphasized that "it is of outmost importance [for] the DLT uses to be compliant with the EU legislation on data protection" and calls on the European Commission and the European Data Protection Supervisor (EDPS) to provide for further guidance on this point. After all, one seems to have recognized the problem that there may be some risk that the EU closes itself off from the future of the internet with respect to BCT. The EU Blockchain Observatory and Forum that has been launched by the Commission with the purpose of mapping key initiatives, monitoring developments, and inspiring common actions held a workshop on June 8, 2018 to examine the clashes and correlations between BCT and GDPR, and to provide, as far as possible, some guidance to technologists, lawyers, entrepreneurs, and citizens in that respect, thus echoing the ITRE's resolution on DLT and BCT. The workshop discussed separately the topics of technical, governance, and legal solutions and came to the positive result that there are only a few questions left unanswered or on which no agreement could be reached. This indicates that the reform of the GDPR is not the silver bullet, especially since the mills of

---

70 Cf., e.g., CZESCHIK & STAMBOLIJA, supra note 8, at 34-38.

71 FINCK, supra note 42, at 29.

72 See for examples and use cases of BCT in the healthcare system CZESCHIK & STAMBOLIJA, supra note 8, at 25-31; NICHOL, supra note 8, at 115-47.

73 Toth, supra note 50.

74 PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE, 5 and passim (2018).

75 European Parliament Committee on Industry, Research and Energy (ITRE), Motion for a resolution on distributed ledger technologies and blockchains: building trust with disintermediation, ITRE/8/10 - 2017/2772(RSP) (Compromise Amendments).

Brussels grind slowly. Rather, it seems to be the order of the day that regulators and officials and BCT parties and developers cooperate towards mutually acceptable solutions such as off-chain storage of personal data and technical work-arounds. Furthermore, the creation of a code of conduct for BCT in accordance with Article 40 of the GDPR might be useful.[76]

Of course, the message that GDPR and BCT can co-exist holds also true for healthcare settings. Consequently, the question may arise what EU initiatives exist specifically for the health sector. The ITRE resolution notes that DLT allows citizens to control and have transparency on their health data, chose which of those data to share, including their use with insurance companies and the wider healthcare ecosystem, but stresses also the necessity to protect the privacy of the sensitive health data.[77] According to the European Commission's communication on "Enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society", published on April 24, 2018, it is intended to monitor the implementation of the GDPR and the eIDAS Regulation[78] with regard to health and to take account of emerging technologies such as blockchain in the context of cybersecurity.[79] That makes sense, as in a decentralized BCT ransomware attacks on hospitals etc. would become more difficult.[80] Furthermore, the Staff Working Document accompanying the Commission's communication expresses the expectation that new emerging cybersecurity solutions building on trusted DLT for protecting the access to personal health data such as BCT could play an essential role if implemented systematically across Europe as part of the national and EU level data and computation infrastructures for personalized medicine.[81] However, this is insufficient in the light of the unsettled legal issues discussed above. Therefore, it remains to be hoped that the Commission, in its announced recommendation on the technical specifications for an EHR exchange format,[82] will take the opportunity to clarify the tension-loaded relationship between BCT and GDPR, thereby creating greater legal certainty.

---

76 BLOCKCHAIN BUNDESVERBAND, supra note 42, at 9.

77 European Parliament Committee on Industry, Research and Energy (ITRE), supra note 75.

78 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257 of 28.8.2014, p. 73).

79 COM(2018) 233 final, 6.

80 Gordon, Wright & Landman, supra note 5; SCHUMACHER, supra note 8, at 4.

81 COMMISSION STAFF WORKING DOCUMENT, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 final, SWD(2018) 126 final, 41.

82 See COM(2018) 233 final, 7.