

## Blockchain meets Data Privacy (Part 1)

### Blockchain and the Data Controller

Dr. Jörg Kaufmann, Lawyer, Waldenberger Rechtsanwälte

07. August 2018

LR 2018, Seiten 120 bis 127 (insgesamt 8 Seiten)

---

Blockchain technology and the General Data Protection Regulation (GDPR) have both received considerable media attention. The GDPR was created against a backdrop of centralized data processing and does not take decentralized approaches such as blockchain into account. Accordingly, blockchain protocols and implementations pose significant challenges to the application of the GDPR. Notwithstanding, blockchain technology can also be seen as a means of data protection.

1

This three-part essay explores the application of the GDPR to blockchain-based data processing. Part one deals with the question of determining the data controller in blockchain systems because numerous responsibilities rest upon the data controller under the GDPR. This regulation is based on the assumption that there is always a data controller behind any processing of personal data. However, the data protection concept of 'control' does not accord with very notion of decentralized data processing.

2

#### I. Introduction

##### 1. Blockchain basics

A blockchain is an open ledger that can record transactions between two parties in a verifiable and permanent way.<sup>1</sup> The ledger is not stored on a central server, but distributed among the participating nodes.<sup>2</sup> The nodes form a peer-to-peer network. A continuously growing list of blocks are linked and secured using cryptography. Each block stores the hash value of the previous block, a timestamp and transaction data. The miners generate hash values for individual blocks by solving complex mathematical problems.<sup>3</sup>

3

---

<sup>1</sup> *Iansiti/Lakhani*, The Truth about Blockchain, Harvard Business Review 95, no. 1 (January–February 2017), 118, <https://hbr.org/2017/01/the-truth-about-blockchain>, (all websites last accessed on August 31, 2018).

<sup>2</sup> *Martini/Weinzierl*, NVwZ 2017, 1251.

<sup>3</sup> *Erbguth/Fasching*, ZD 2017, 560, 563.

Blockchains rely on asymmetric cryptography. The private key of a participant is used to sign a transaction whereas the public key serves to confirm the signature.<sup>4</sup>

According to Don Tapscott blockchains have the potential to revolutionize the world economy.<sup>5</sup> Use cases have been identified in the following sectors: banking, fintech, insurance, Internet of things (IoT), data security, energy, e-government, mobility and legal tech.<sup>6</sup> Blockchains can form the basis of cryptocurrencies, machine-to-machine (M2M) communication, decentralized autonomous organizations (DAO) and smart contracts.<sup>7</sup>

## 2. Types of blockchain

The term 'blockchain' can be used to describe various technological approaches.<sup>8</sup> There is a difference between public and private blockchains. In a public blockchain scenario, the access to the network and to reading transaction data is not restricted.<sup>9</sup> In contrast, the participation in a private blockchain requires prior authorization.<sup>10</sup> There is also a difference between permissionless and permissioned blockchains. Each node may confirm transactions in a permissionless blockchain context<sup>11</sup>, even though the mining process requires significant computational resources. In a permissioned blockchain environment only authorized nodes may undertake the mining process.

The blockchain underlying the Bitcoin network is public and permissionless.<sup>12</sup> Anybody can download the client software, gain access to the network and verify transactions. Private and permissioned blockchains are popular among banks and insurance companies, but here the original blockchain idea has been adapted towards the specific needs of these financial sectors.<sup>13</sup> For example, their blockchains, such as the private and permissioned R3 Corda network, do not implement the idea of radical transparency.

<sup>4</sup> Kaulartz, CR 2016, 474, 475.

<sup>5</sup> Tapscott, How blockchains could change the world, McKinsey & Company, May, 2016,

<https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world>.

<sup>6</sup> Voshmgir, Blockchains, Smart Contracts und das Dezentrale Web, Technologiestiftung Berlin, January 30,

2017, [https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130\\_BlockchainStudie.pdf](https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf), 17.

<sup>7</sup> Kaulartz, CR 2016, 474.

<sup>8</sup> Kunde/Kaulartz/Naceur/Liban/Kunz/Skwarek/Adam/Weiß/Liesenjohann, Faktenpapier Blockchain und Datenschutz, bitkom, January 24, 2018, <https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html>, 8.

<sup>9</sup> Breidenbach/Glatz, Rechtshandbuch Legal Tech, 2018, 69, rec. 35.

<sup>10</sup> Kunde/Kaulartz/Naceur/Liban/Kunz/Skwarek/Adam/Weiß/Liesenjohann, Faktenpapier Blockchain und Datenschutz, bitkom, January 24, 2018, <https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html>, 9.

<sup>11</sup> Maxwell/Salmon, A guide to blockchain and data protection, Hogan Lovells, September 2017, <https://www.h lengage.com/uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf>, 17.

<sup>12</sup> Blockchains & Distributed Ledger Technologies, Blockchain Hub, <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general>.

<sup>13</sup> Breidenbach/Glatz, Rechtshandbuch Legal Tech, 2018, 69, rec. 36.

## II. The General Data Protection Regulation

The General Data Protection Regulation (GDPR) has, just like blockchain, received considerable media attention. There is, however, hardly any innovative potential in this regulation, which is based on recycled concepts of data protection law.<sup>14</sup> Thomas Hoeren, a professor of law at the University of Münster and a former Court of Appeal Judge, has described the GDPR 'as one of the worst laws in the history of the 21<sup>st</sup> century'.<sup>15</sup> Companies and organizations see the new regulation as little more than a cumbersome compliance issue which has to be dealt with in order to avoid drastic fines.

7

Recital 15 par. 1 GDPR declares that it takes a technology-neutral approach towards data protection. Accordingly, the regulations are the same for social networks, cloud storage providers, online retailers and blockchain-based implementations. This is because the GDPR was created against a backdrop of centralized data processing, with the result that it does not take decentralized technologies into account. This failure to pay attention to the complexities of technological applications results in several problems for the practical application of the GDPR, and in particular, to blockchain-based data processing. In fact, the new regulation is not 'technology neutral.' Rather, it places decentralized data processing at a competitive disadvantage.<sup>16</sup>

8

## III. Personal data on a blockchain

The General Data Protection Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data, as well as rules relating to the free movement of personal data (art. 1 par. 1). This means that the applicability of data protection law is based on the involvement of personal data.<sup>17</sup> Yet what is 'personal data'? The GDPR defines it as any information relating to an identified or identifiable natural person (art. 4 no. 1). However, there has been much debate over the putative 'identifiability' of a natural person behind certain data.<sup>18</sup> This 'identifiability' should nevertheless be assumed as long as it cannot be excluded with certainty.<sup>19</sup> Accordingly,

9

---

<sup>14</sup> *Härting*, GDPR: Heaven for Lawyers, CR-online.de Blog, May 4, 2018, <https://www.cr-online.de/blog/2018/05/04/gdpr-heaven-for-lawyers>.

<sup>15</sup> *Krempf*, Rechtsexperte: Datenschutz-Grundverordnung als "größte Katastrophe des 21. Jahrhunderts", heise online, April 27, 2016, <https://www.heise.de/newsticker/meldung/Rechtsexperte-Datenschutz-Grundverordnung-als-groesste-Katastrophe-des-21-Jahrhunderts-3190299.html>.

<sup>16</sup> *Eichler/Jongorius/McMullen/Naegele/Steininger/Wagner*, Blockchain, data protection, and the GDPR, Blockchain Bundesverband, May 25, 2018, [https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR\\_Position\\_Paper\\_v1.0.pdf](https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf), 2.

<sup>17</sup> *Härting*, DSGVO, 2016, rec. 262.

<sup>18</sup> *Herbst*, NVwZ 2016, 902.

<sup>19</sup> *Härting*, DSGVO, 2016, rec. 267; *Schreiber/Kollmar*, *Härting*, Was Blockchain mit Datenschutz zu tun hat, March 7, 2018, <https://www.haerting.de/neuigkeit/was-blockchain-mit-datenschutz-zu-tun-hat>.

name, email address, telephone number, IP-address, and so forth, all qualify as personal data.

This leads to the question as to whether the data that is processed by blockchain networks can be considered personal data. As the administrator of a private blockchain grants access to the network, his or her position is similar to that of an Internet service provider. The administrator can easily link a public key to a specific natural person, meaning that the participants of a private blockchain are easily identifiable.<sup>20</sup> According to art. 4 no. 1 GDPR, therefore, data which is processed by private blockchains qualifies as personal data.

10

A public blockchain, however, does not store information such as names or addresses.<sup>21</sup> Rather, it keeps a record of hash values, public keys and other transaction data. The stored information is usually sufficient to identify the blockchain participant with the help of data analytics tools.<sup>22</sup> The identification of the blockchain user is even simpler if he or she reveals the public key when using a cryptocurrency marketplace<sup>23</sup> or wallet. It is recommended, therefore, that participants use a different public key for each transaction, although it is still possible to identify the user behind each of the various public keys.<sup>24</sup> Hence, public blockchains do in fact process personal data in accordance with art. 4 no. 1 GDPR.

11

## IV. Data controllership

### 1. The role of the data controller

According to art. 4 no. 7 GDPR, the ‘controller’ is the natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of the processing of personal data. Where two or more controllers jointly determine the purposes and means of processing they shall be considered ‘joint controllers’ (Art. 26 par. 1 GDPR). Art. 4 GDPR also defines the ‘processor’ and the ‘data subject’. The ‘processor’ is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art. 4 no. 8 GDPR). The ‘data subject’ is an identified or identifiable natural person whose personal data is being processed (Art. 4 no. 1 GDPR).

12

<sup>20</sup> Schrey/Thalhofer, NJW 2017, 1431, 1433.

<sup>21</sup> Hofert, ZD 2017, 161, 163.

<sup>22</sup> Martini/Weinzierl, NVwZ 2017, 1251, 1253.

<sup>23</sup> Kunde/Kaulartz/Naceur/Liban/Kunz/Skwarek/Adam/Weiß/Liesenjohann, Faktenpapier Blockchain und Datenschutz, bitkom, January 24, 2018, <https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html>, 21.

<sup>24</sup> Erbguth/Fasching, ZD 2017, 560, 562.

Art. 5 par. 2 GDPR assigns 'accountability' to the data controller. In addition, the data subject must exercise his or her rights mainly vis-à-vis the controller. For example, according to art. 16 GDPR, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her ('right to rectification'). Art. 17 par. 1 GDPR states that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay under certain circumstances ('right to erasure'). 13

## 2. Centralized data processing & the data controller

Art. 4 GDPR defines very precisely the different players involved in data processing. These definitions are based on the centralized data processing model.<sup>25</sup> For example, if a consumer buys a product online, then he or she will provide the online retailer with personal data, such as name, email address, and bank details. The consumer might also consent to the processing of his or her personal data for one or more specific purposes (art. 6 no. 1 (a) GDPR). The consumer may not read the declaration of consent, but simply accept it by ticking the appropriate box. This means that the consumer may not necessarily know in greater detail in what ways, and for which purposes, his or her personal data will be processed by the online retailer. In this example, the online retailer is the controller and the customer is the data subject. Yet there may also be data processors who process the consumer's personal data on behalf of the online retailer. 14

## 3. Blockchain systems & the data controller

The definition of the data controller, according to art. 4 no. 7 GDPR, is, however, more difficult to apply to the storage and processing of personal data by blockchain technology because it is decentralized. In a decentralized blockchain environment, there is no single person or organization that determines single-handedly the purpose and means of the processing of personal data.<sup>26</sup> Yet data privacy law is based on the assumption that there is always a data controller behind any processing of personal data (rec. 79 GDPR). In order to properly determine the data controller, it is necessary to consider the different players within the particular blockchain application, as well as its specific characteristics.<sup>27</sup> 15

<sup>25</sup> Schreiber/Kollmar, Härting, Was Blockchain mit Datenschutz zu tun hat, March 7, 2018, <https://www.haerting.de/neuigkeit/was-blockchain-mit-datenschutz-zu-tun-hat>.

<sup>26</sup> Erbguth/Fasching, ZD 2017, 560, 563.

<sup>27</sup> Kunde/Kaulartz/Naceur/Liban/Kunz/Skwarek/Adam/Weiß/Liesenjohann, Faktenpapier Blockchain und Datenschutz, bitkom, January 24, 2018, <https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html>, 28.

## a. Public/permissionless blockchains

### aa. Software developers

With the release of the software code, the developer of a public/permissionless blockchain effectively relinquishes control of the purposes and means of the processing of personal data.<sup>28</sup> Similar to other programmers, blockchain developers only supply a means for the processing of personal data, even though occasionally they play an important role in the further technical advancement of the blockchain.<sup>29</sup> Nonetheless, solving technical problems is not considered as a determination of the purposes and means of the processing of personal data by the blockchain system.<sup>30</sup> The developers of blockchain protocols or implementations are therefore not data controllers under the GDPR.

16

### bb. Miners

Miners, on the other hand, make a major contribution to the functioning of the blockchain network by confirming transactions.<sup>31</sup> These stakeholders cannot, however, influence the transaction data within the individual blocks. If a miner tried to manipulate transactions, the false data would be rejected by the other miners.<sup>32</sup> A group of miners which combine more than fifty percent of the computational power of the network would technically be in a position to control the transactions on the blockchain, although mining pools try not to reach such a share of computing power.<sup>33</sup> In general, therefore, miners do not determine the purposes and means of the processing of personal data in a blockchain system. Rather, they are confined to the role which has been assigned to them in the blockchain protocol. Under the GDPR, therefore, miners are not data controllers.

17

### cc. Nodes

A node is a computer which has installed a software that runs the blockchain protocol. If the node does not adhere to the rules of the protocol, it will be ignored by the rest of the network.<sup>34</sup> Accordingly, a single node is not in a position to determine the purposes and means of the processing of personal data on the blockchain. By contrast, the entire group of nodes would be in full control of the blockchain network and the processing of personal

18

<sup>28</sup> *Martini/Weinzierl*, NVwZ 2017, 1251, 1253.

<sup>29</sup> Castillo, Ethereum Executes Blockchain Hard Fork to Return DAO Funds, coindesk, July 20, 2016, <https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds>

<sup>30</sup> *Martini/Weinzierl*, NVwZ 2017, 1251, 1253.

<sup>31</sup> *Kunde/Kaulartz/Naceur/Liban/Kunz/Skwarek/Adam/Weiß/Liesenjohann*, Faktenpapier Blockchain und Datenschutz, bitkom, January 24, 2018, <https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html>, 28.

<sup>32</sup> *Erbguth/Fasching*, ZD 2017, 560, 563.

<sup>33</sup> *Hajdarbegovic*, Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack, coindesk, January 9, 2014, <https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack>.

<sup>34</sup> *Erbguth/Fasching*, ZD 2017, 560, 563.

data. This raises the question of joint controllership according to art. 26 GDPR, which requires a joint agreement on the processing of personal data. Such agreements do not exist, however, in a public/permissionless blockchain system.<sup>35</sup> Neither a single node nor the entire group of nodes can therefore be considered as a data controller under the GDPR.

#### **dd. Participants**

A participant running a node interacts directly with the public/permissionless blockchain. He or she decides single-handedly on the exact amount of cryptocurrency that will be sent from his or her public key to the receiver's public key.<sup>36</sup> The transaction data will be stored on the blockchain and cannot be erased afterwards. Therefore, one may consider blockchain participants as data controllers.<sup>37</sup> Such a view is oblivious, however, to the decentralized nature of public/permissionless blockchains. There is no single point of control in these blockchains. It would therefore be inappropriate and impractical to assign the burden of data controllership to a single blockchain player. The assumption that there must always be a data controller behind any processing of personal data is unfounded, because 'control' is decentralized in a public/permissionless blockchain. Blockchain participants should not be considered as data controllers under the GDPR, even though this view might not necessarily be shared by supervisory authorities.

19

#### **ee. Exchanges and wallets**

Users of cryptocurrencies may take advantage of exchanges or wallets. An exchange is a website which handles the trading of cryptocurrency to fiat money or other cryptocurrencies.<sup>38</sup> A wallet site is a service that allows users to store their cryptocurrencies. In both cases, the interaction between the user and the blockchain network takes place via the service provider.<sup>39</sup> The provider assumes control over the execution of transactions and/or the storage of cryptocurrencies belonging to the user. Exchanges and wallets, therefore, determine the purposes and means of the processing of personal data. According to art. 4 no. 7 GDPR, they are data controllers vis-à-vis the user of their services.

20

---

<sup>35</sup> *Martini/Weinzierl*, NVwZ 2017, 1251, 1254.

<sup>36</sup> *Erbguth/Fasching*, ZD 2017, 560, 564.

<sup>37</sup> *Schrey/Thalhofer*, NJW 2017, 1431, 1433.

<sup>38</sup> *De la Torre*, Quora, May 25, 2016, What are the differences between a Bitcoin exchange vs a Bitcoin wallet website? <https://www.quora.com/What-are-the-differences-between-a-Bitcoin-exchange-vs-a-Bitcoin-wallet-website>.

<sup>39</sup> *Erbguth/Fasching*, ZD 2017, 560, 564.

## b. Private/permissioned blockchains

The data controller is much easier to determine in private/permissioned blockchains. The administrator of this kind of blockchain grants access to the network,<sup>40</sup> and as such, determines the purposes and means of the processing of personal data on the blockchain.<sup>41</sup> For example, in the sense of art. 26 GDPR, if a group of banks sets up a private/permissioned blockchain, the various banks will be joint controllers. 21

Nodes and miners are generally considered as data processors.<sup>42</sup> However, the assessment depends on the characteristics of the actual private/permissioned blockchain. 22

## 5. Findings

The question of determining the data controller in a blockchain system is subject to an ongoing discussion. To answer this question, the various types of blockchain and their characteristics must be taken into account. As I have shown, determining the data controller in a public/permissionless blockchain system is more difficult than in a private/permissioned environment. However, companies and commercial organizations are most likely to rely on private/permissioned blockchains. Stakeholders in these companies should therefore stay informed about future developments in the application of the GDPR to the processing of personal data by blockchain systems. 23

---

<sup>40</sup> *Kunde/Kaulartz/Naceur/Liban/Kunz/Skwarek/Adam/Weiß/Liesenjohann*, Faktenpapier Blockchain und Datenschutz, bitkom, January 24, 2018, <https://www.bitkom.org/Bitkom/Publikationen/Faktenpapier-Blockchain-und-Datenschutz.html>, 30.

<sup>41</sup> *Martini/Weinzierl*, NVwZ 2017, 1251, 1254.

<sup>42</sup> *Schreiber/Kollmar*, Härting, Was Blockchain mit Datenschutz zu tun hat, March 7, 2018, <https://www.haerting.de/neuigkeit/was-blockchain-mit-datenschutz-zu-tun-hat>.