Conceptualizations of the controller in permissionless blockchains

by **Maurice Schellekens**[*]

Abstract: The relationship between blockchain and the General Data Protection Regulation (hereinafter GDPR) is often described as problematic. This article addresses one of the problems blockchain faces: who is/are the controller(s) in a blockchain context? This article demonstrates that it is particularly difficult to identify the controller in blockchain applications that are integrated in the core code of a permissionless blockchain. The P2P character of blockchains, with its broad distribution of responsibilities, makes it difficult to ascertain who is able to determine purposes and means of the processing of data. In order to structure the discussion, this article develops three conceptualizations of cooperation within a blockchain. These conceptualizations give different perspectives on the relations between the actors in a blockchain that are potential controllers. The article identifies who is most likely to be the controller in the different conceptualizations and gives indications about the extent to which the controllers are able to exercise their responsibilities. A problem is that an adequate exercise of responsibility requires coordination within the blockchain. However, the system that normally takes care of coordination in a permissionless blockchain – the crypto-economic incentive system – is at present not able to provide adequate data protection.

Keywords: Controller; Blockchain; permissionsless Blockchain; GDPR

Recommended citation: Maurice Schellekens, Conceptualizations of the controller in permissionless blockchains, 11 (2020) JIPITEC 215 para 1.

A. Introduction

1 Blockchain is a distributed ledger that introduces a new way of processing data. Data on a blockchain are immutable and storage is independent from the intermediaries, involved in managing the blockchain. There is a – currently unproven - promise of new business models and innovation.

2 Blockchain's relationship with the GDPR is tense, not least because it is difficult to establish accountability in a blockchain. Blockchain's horizontal character is laid out to minimize the influence of individual administrators within the blockchain.

3 The dilution of influence makes it difficult to pinpoint who determines purposes and means of data processing, in other words, who is the controller.

4 This article seeks to bring the discussion regarding accountability a step further by discerning three ways of conceptualizing the relations or cooperation between the actors in a blockchain context.

5 This article proceeds as follows. In the next section, blockchain technology will be explained for the purposes of this article. The following section analyses controllership and presents the conceptualizations of the relations amongst relevant actors. The fourth section is the conclusion.

B. Blockchain technology

I. Distributed database

6 A blockchain is in essence a distributed database, i.e. a database of which multiple copies exist. Every copy is stored on a computer within a network (a node) and each node has an administrator. If new data or transactions are added to the blockchain, they are first collected in a so-called block and are then en bloc appended to the end of the existing blockchain. The newly added block has a pointer (a hash) linking it to the last block in the existing chain.

7 The Bitcoin blockchain is the architype blockchain and this has shaped how we see a blockchain. The basic processes of the Bitcoin blockchain are adopted in other blockchains, such as Ethereum. The Bitcoin blockchain was first described in Satoshi Nakamoto's paper of 2008, entitled: "Bitcoin: A Peer-to-Peer Electronic Cash System". [1] In his paper, Nakamoto identifies the immutability of the data that the blockchain contains as its core characteristic. Here, "immutability" means that once data has been added to the blockchain, it can no longer be changed or deleted from the blockchain, not even by the administrator of a node who added the data to the block. The reason Nakamoto strives for immutability is to obviate trust in the administrator or any other actor that may persuade the administrator to alter or remove data from the database. Nakamoto's paper appeared during the financial crisis of 2008 when trust in banks was at a low point. Bitcoin, which is a crypto-currency, was meant to create internet money that could function without an intermediary, like a bank. All previous attempts at creating internet money needed an intermediary to prevent double spending. The Bitcoin blockchain claims to have made trust in intermediaries redundant. The questions regarding whether a blockchain really succeeds in doing so and whether that is a useful property at all, will not be addressed here. This section of the article focuses on the question of how immutability of the contents of the database is realized.

8 A first means to create immutability is redundancy. As stated above, there exist multiple copies of the database under the control of various administrators. Redundancy reduces the dependence on each individual node administrator. In ways that will become apparent below, an alteration or deletion of data on the blockchain by one administrator will not affect what is seen as the valid blockchain.

9 A second means to create immutability is reliance on crypto-economic incentives. There are positive and negative incentives to make the administrators of nodes play by the rules of the game (i.e. the protocol). A positive incentive is that an administrator can earn bitcoins by playing by the rules. A negative incentive is that an administrator first has to invest (for example in computer equipment and electricity) in order to be able to earn bitcoins. If the administrator does not adhere to the protocol, his investment will be in vain.

10 The redundancy and crypto-economic incentives work towards immutability of the contents of the blockchain in ways that will become apparent below. At the same time, the existence of multiple copies (or perhaps better versions) of the database creates a new problem, namely the risk that they will exhibit differences in the data they register. In other words, there is a need to sync the versions. This requires coordination within the blockchain. A traditional way to create such coordination is to designate one database as the master and all other databases as the slaves that have to follow the master at all times. This would however re-introduce centralization, dependence on the master database, and trust in its administrator, which Nakamoto deems undesirable. So the challenge is to create coordination while maintaining decentralization. A first step in creating coordination is the definition of what counts as the valid blockchain; this is defined as the longest chain consisting purely of valid blocks. How a valid block is defined will become apparent below.

11 The way in which new blocks are added to the blockchain elucidates how the coordination can be achieved while maintaining decentralization.[2] During a period of about ten minutes, each node collects new transactions (new data to be added to the blockchain) and places them in a candidate-block. Each node prepares his own candidate block. He checks all incoming transactions on double spending by comparing the transactions to the contents of the blockchain. The node includes in his candidate-block a reference to the last block of what he thinks is the longest existing chain. At the end of the ten-minute-period, the candidate blocks are finalized and the nodes start solving a cryptographic puzzle based on their candidate blocks. They compete against each other to be the first to solve their puzzle. The first node to solve his cryptographic puzzle, sends his Proof-of-Work (i.e. the proof he solved his puzzle) to all the other nodes, who then verify that our node

* Senior researcher at Tilburg Institute for Law, Technology, and Society, Tilburg University.

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' [2008] 1 <https://bitcoin.org/bitcoin.pdf> accessed 6 June 2019.

[2] Andreas M Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* (O'Reilly Media 2017) ch 2.

solved his cryptographic puzzle. If they are satisfied that he did so, they accept the candidate block of the winner as the new block that they add to the blockchain. An administrator does so by including a reference to this block in his new candidate block. In other words, an administrator indicates what the valid chain is by building on it. The duration of the ten minute period derives from the time it costs with the most advanced computers to solve the cryptographic puzzle. So, while a node is solving the crypto-graphic puzzle based on his candidate for the n-th block (costing about ten minutes), he is already collecting new transactions for his (n+1) th block during the same ten minutes. Once some node has found proof-of-work for the n-th block, immediately a new competition starts for proof-of-work of the (n+1)th block. A valid block is a block for which proof-of-work exists and that contains only valid transactions. Each node has written a sort of cheque to itself into its candidate block and only the winning node can cash in on this cheque, since only its own block is added to the blockchain that is considered valid.

12 This all creates a blockchain that is immutable in the sense described above. This can be seen as follows. Suppose that a node changes the contents of an old block somewhere in the middle of the chain. Then, the proof-of-work of this block is no longer valid and also the reference in the subsequent block to the modified block is no longer correct. This means that the chain of our node is broken. It is no longer the longest chain and will be ignored by the other nodes: they can only earn bitcoins by building on the longest chain. So, changing data in an old block is strongly discouraged. It disqualifies the administrator for meaningful participation in the blockchain.

13 The above describes how the bitcoin blockchain works. The Bitcoin blockchain is a so-called permissionless blockchain. This means that everybody can become a node mining for a reward. Nobody needs “admission” to become a node. Permissionless blockchains work with crypto-economic incentives of which the above are an example.[3] A node is not bound by contract or another legal instrument. Another example of a blockchain with miners is Ethereum 1.0.

II. Proof-of Stake

14 Although the Bitcoin blockchain is sometimes seen as an outlier in its rejection of legal instruments as sources of trust, other more mainstream or business oriented blockchains, such as Ethereum, work with the same technical concept.[4] Ethereum has until now relied on Proof-of-Work, just as Bitcoin. However, Proof-of-Work exhibits certain shortcomings in terms scalability and sustainability. Therefore, Ethereum seeks to switch to an alternative technical concept, Proof-of-Stake. Where miners commit computer equipment and electricity, validators in Ethereum 2.0 commit Ether, i.e. the cryptocurrency of Ethereum. Under the envisaged Proof-of-Stake mechanism, the next block to add is chosen through voting. The vote of a validator is weighed according to the amount of Ether he has committed (the stake). Since the validators cannot trust each other and since they communicate over an unsafe network (the internet), fraud is a problem.[5] This requires Ethereum to take measures to prevent fraud, to detect it and to redress it, e.g. by finding ways to automatically “slash” the stake of fraudulent validators. Even though Ethereum has often announced dates at which the switch to Proof-of-Stake would take place,

[3] There are also so-called permissioned blockchains. In order to become a node in a permissioned blockchain a person needs to be admitted. Sometimes a central party is charged with admissions. It can also be that the collective of existing node administrators decides about new admissions. A permissioned blockchain can also work with crypto-economic incentives. It may however be that such a blockchain works with a simpler coordination mechanism, such as a round-robin system; each node in turn delivers a new block (BitFury Group in collaboration with Jeff Garzik, ‘Public versus Private Blockchains. Part 1: Permissioned Blockchains’, White Paper, 20 October 2015 (Version 1.0), 5). In the latter case, it is also easy to accommodate a procedure to modify the contents of old blocks. This is the reason that some do not consider these permissioned blockchains to be blockchains at all.

[4] Alyssa Hertig, ‘How Ethereum mining works’ (*Ethereum 101*) <https://www.coindesk.com/learn/ethereum-101/ethereum-smart-contracts-work> accessed 4 May 2020.

[5] In this context, inter alia the nothing-at-stake attack, the long range attack and an attack by a cartel can be mentioned. See Vlad Zamfir, ‘The history of Casper’ (*Ethereum blog,* 6 December 2016) ch 1,2 and 5. <https://blog.ethereum.org/2016/12/06/history-casper-chapter-1/> accessed 4 May 2020.

the switch has – at the moment of writing – not materialized and Proof-of-Work remains relevant for the time being.

III. Smart contracts

15 Above we considered that data (e.g. bitcoin transactions) are stored on a blockchain. In the (permissionless) blockchain Ethereum, users can place code on the blockchain. The code placed on the blockchain is immutable in the same way that data on the blockchain are immutable.[6] Moreover, the code can be executed by the nodes if some (other) user seeks to do so. For example, a hotel may place code on a blockchain that opens an IoT hotel room door after the code has checked that the hotel guest has paid for the night.[7] Such code is called a smart contract.[8] One must however bear in mind that a smart contract is simply code. It is not said that the code forms a contract in the legal sense, even though many applications, such as the example above, are in a domain that is reminiscent of contracts. It is also not said that a smart contract is smart in the sense that it uses artificial intelligence or something along the same lines. The example above is illustrative again. The smart contract may typically function as a trusted middle man.

IV. ICOs

16 A popular application of permissionless blockchains is an Initial Coin Offering (hereinafter ICO). It is a means of crowdfunding whereby newly issued tokens are sold to investors or speculators in exchange for legal tender or cryptocurrencies.[9] Most ICOs are built on the Ethereum platform. This platform is popular, since an ICO can easily be programmed as an Ethereum smart contract and the standardization of certain aspects of tokens within Ethereum allows for the tradability of the tokens.[10] There are various types of tokens that can be issued. Usually a distinction is made between utility tokens and equity tokens.[11] A utility token gives the holder the right to buy in the future certain products or services from the issuer. This is typically the product or service developed with the capital that the ICO yields. An equity token gives the holder certain rights that can be exercised against the issuing company, such as a right to profits generated or a share in the residual value if and when the company is liquidated. Although this article is not the place to discuss whether an ICO is subject to financial regulations, it can be said that some ICOs will indeed

[6] In order to address concerns about the immutability of smart contracts, the function 'delegatecall' has been developed. A call of an undesired smart contract can be relayed to another contract. Merunas Grincalaitis, 'Can a Smart Contract be upgraded/modified? Is CPU mining even worth the Ether? The Top questions answered here…', (*Medium*, 6 February 2018) <www.medium.com> accessed 6 June 2019.

[7] Vitalik Buterin, 'DAOs, DACs, DAs and More: An Incomplete Terminology Guide' *(Ethereum Blog,* 6 May 2014) <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/> accessed 21 October 2019.

[8] Term coined by Szabo in: Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets', 1996 <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 6 June 2019. It predates blockchain.

[9] Patrick Schueffel, 'The Concise Fintech Compendium', (School of Management Fribourg (HEG-FR)), <https://web.archive.org/web/20180425130029/http://www.heg-fr.ch/FR/HEG-FR/Communication-et-evenements/evenements/Documents/Schueffel2017_The-Concise-FINTECH-COMPENDIUM.PDF> accessed 4 May 2020, gives a more restrictive definition: 'An ICO is an unregulated means of crowdfunding applied by cryptocurrency businesses as an alternative to the rigorous and regulated capital-raising process required by venture capitalists, banks, or stock exchanges. In an ICO a percentage of the newly issued cryptocurrency is sold to investors in exchange for legal tender or other cryptocurrencies such as Bitcoin.'

[10] Almost 57% of ICOs builds on Ethereum smart contracts. Almost 30% of the ICOs works with a dedicated blockchain for the ICO. Source: <https://web.archive.org/web/20171230074510/https://icowatchlist.com/blog/ico-market-research-leading-blockchain-platforms-2017/> accessed 4 May 2020. Gianni Fenu, Lodovica Marchesi, Michele Marchesi and Roberto Tonelli, 'The ICO Phenomenon and Its Relationships with Ethereum Smart Contract Environment' [2018] IEEE <https://www.researchgate.net/publication/324099008_The_ICO_phenomenon_and_its_relationships_with_ethereum_smart_contract_environment/link/5db84e6ca6fdcc2128eb86e1/download> accessed 3 May 2020. Romi Kher, Siri Terjesen and Chen Liu, 'Blockchain, Bitcoin, and ICOs: a review and research agenda' [2019] Small Bus Econ, Springer <https://doi.org/10.1007/s11187-019-00286-y> accessed 3 May 2020.

[11] J. Baukema, 'Initial Coin Offerings (ICO's): crowdfunding 2.0?' (2018) (3) Tijdschrift voor financieel recht, 113 <https://www.vandoorne.com/globalassets/documenten--bijlagen/publicaties/2018/j.-baukema---icos.pdf> accessed 4 May 2020.

be caught by such regulation.[12] This is relevant for the discussion about data protection below, since it can trigger KYC and AML obligations.[13]

V. Actors in a blockchain

17 Many actors are involved in blockchains. For the purpose of this article the following are discerned. The core developers develop the code that constitutes the blockchain. There are administrators of nodes. In the description above they solve cryptographic puzzles, they store a version of the entire blockchain and check transactions. Often these tasks are however divided over two types of node administrators. On the one hand, there are miners who solve cryptographic puzzles or validators who vote, and on the other hand, there are administrators of so-called full nodes: they store an entire copy of the blockchain and check transactions. Users are the actors that place transactions or smart contracts on the blockchain. Finally, there are so-called oracles. They provide information that is not yet readily available in the blockchain. For example, if two parties bet via a blockchain on the temperature in London tomorrow the blockchain may derive information about the temperature from the website of the British Broadcasting Corporation (BBC). The BBC then acts as an oracle for the blockchain.

18 A distinction can be made between the infrastructure level and the application level. At the infrastructure level, you find the core code that constitutes the blockchain. At the application level you find smart contracts, i.e. user inserted code. However, this distinction is marred somewhat by the fact that a cryptocurrency is infrastructure level (coded by the core developers and needed to make the consent mechanism function), but it feels like an application as well. For those making payments with Bitcoin, it clearly functions as an application. A permissionless blockchain is always public. This means that everybody can read the data or smart contracts stored on the blockchain.

C. Blockchain and the GDPR

19 The GDPR is applicable to the processing of personal data. For an analysis of blockchains, this implies that relevant instances of processing of personal data need to be identified and asked whether the data involved are personal data for the actors who are potential controllers. Subsection C.I below addresses these questions.

20 In literature, it is argued that the GDPR is unfit for application to blockchains.[14] Blockchain's peer-to-peer character would not sit well with the conceptual idea about processing of data underlying the GDPR, namely the idea of a centralized database with a clear administrator. Hereinafter in subsections C.II and C.III, this article will investigate how blockchain's P2P character relates to who should be considered data controller and data processor.

I. Personal data

21 Participation in the Bitcoin blockchain happens via digital signatures, a pair of private and public keys. The public keys of those participating in a transaction are stored in the public blockchain. To prevent more than two transactions being linked together, participants change their digital signature as often as possible.[15] This should make it difficult for a party to be singled out in the blockchain and identified by combination with other information. This may even be effective, unless a party seeking identification has very powerful analysis tools. Typically, only law enforcement and security services would be in a position where motive, and analytical capacity come together to engage in such an identification endeavor. Nonetheless, it cannot be excluded that also other parties, and especially potential controllers such as users and full nodes, can arrive at an identification.

22 First, a user who engages in a transaction with another party may know the identity of the other party or at least have background information that makes identification more likely. After all, transactions do not take place in complete social vacuum.

23 Second, full nodes do receive the transactions via the internet. This gives access to IP addresses from which transactions are sent. Usually a full node will not be able to infer an identity from an IP address. Since the decision of the CJEU in the Breyer case, it is clear that information available to a third party may come in the ambit of means reasonably likely to be used, unless the effort needed to access it would be disproportionate and "the risk of identification

[12] Baukema (n 12) 119-120.

[13] Baukema (n 12) 120 mentions the example of an issuer of tokens that can be found to be an investment institution.

[14] Meyer (n 1). Finck (n 1) 88.

[15] The transaction in which a 'bitcoin' is received is linked to the transaction in which it is spent again.

appears in reality to be insignificant”.[16] Given that illegal content may be stored on a blockchain e.g. via a bitcoin transaction,[17] a full node can have an interest in knowing who placed illegal information on the full node’s system. This would require cooperation from an internet provider who can link the IP address to an identity legally. A claim to obtain personally identifying information of the person who placed the content on the blockchain from the pertinent Internet Provider has a good chance of being found proportional.[18] The immutability of the blockchain makes removal of content from the blockchain extremely costly for the full node. Therefore, being able to address the uploader is an important means to prevent or discourage illegal content upload from re-occurring in the future.

24 Above, it was indicated that an issuing company in an ICO may be required to collect KYC-information and in practice, KYC information is indeed collected.[19] KYC obligations require identification of the customer or its beneficial owner.[20] Given the smaller amounts that can be paid into an ICO, the customer or the beneficial owner will often be a natural person. Therefore, KYC information will often consist of personal data.

II. The data controller

25 The GDPR defines the controller as the person who “determines the purpose of and means for processing personal data”.[21] In a blockchain context, often a central party can be distinguished who is responsible for offering a service. This party will also be considered to be the controller within the meaning of the GDPR, assuming that the service includes the processing of personal data. This party chooses the purpose (the service) and the means (e.g. a smart contract). For example, if a company collecting capital via an ICO uses a smart contract to code the ICO, it can itself be regarded as the controller since it determines purpose (ICO) and means (blockchain-based smart contract). If KYC obligations apply to the ICO, the issuing company processes the data that need to be collected. If a custom made blockchain is used for the ICO (which is rather the exception) in essence the same holds. Another example is an insurer that offers a form to claim for damages through a smart contract.[22] The insurer is responsible for the processing of personal data in the completed forms. An oracle that provides personal data to a smart contract will generally also be considered responsible for the delivery of personal data. Whoever offers a service will usually be apparent from the service on offer. For example, the person who presents himself as a service provider in a smart contract. If a service is offered anonymously, the identification of who is offering the service needs to look at other elements. Whoever has placed the smart contract on the blockchain could be an indication of this. Although blockchain considers decentralization to be of paramount importance, it is often possible to identify a central party that can function as a controller, in particular where the application is coded in Ethereum smart contracts.

1. More challenging cases

26 If the “application” is part of the core code, it is more challenging to find out who the controller is. Who is the controller of bitcoin transactions for example? The core developers are responsible for the code that constitutes the blockchain and its native

[16] Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779, para 46.

[17] Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Mullmann, Oliver Hohlfeld, and Klaus Wehrle, ‘A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin’, to appear in Proc. 22nd International Conference on Financial Cryptography and Data Security 2018. Proceedings to be published via Springer LNCS: <http://www.springer.de/comp/lncs/index.html>, <https://www.comsys.rwth-aachen.de/fileadmin/papers/2018/2018_matzutt_bitcoin-contents_preproceedings-version.pdf> accessed 4 May 2020.

[18] Case C275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, ECLI:EU:C:2008:54, para 70.

[19] See <www.topicolist.com> accessed 7 May 2020.

[20] Art. 13 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L156/43.

[21] Art. 4 sub 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) [2016] OJ L 119/1.

[22] Example borrowed from CNIL, *Blockchain. Premiers* éléments *d’analyse de la CNIL* (Sept. 2018).

cryptocurrency. They are however not involved in the day-to-day running of the blockchain. We will consider their role below.

27 That leaves us with the users and the administrators of nodes as potential data controllers in permissionless blockchains. However, it is not so easy to see who amongst them is a data controller and why. It depends very much on how their roles and mutual relations are perceived. Hereinafter, we discern three conceptualizations that represent three alternative views on permissionless blockchains and on the relationships amongst the main actors involved in the operation of the blockchain. The conceptualizations help to unravel some of the confusion that exist around permissionless blockchains and controllership under the GDPR. In a first conceptualization, the emphasis is on the users that together form a P2P network. In a second conceptualization, the full nodes together offer a service, and in in the third conceptualization each full node is seen as an individual service provider.

a) The users form a P2P network with each other

(aa) What is the conceptualization?

28 This conceptualization closely follows the argumentation of Nakamoto. Users deal with each other without reliance on potentially untrustworthy intermediaries. If A pays bitcoins to B, A and B deal with each other directly. The administrators of automated nodes in between are discarded from the picture. The system of crypto-economic incentives ensures that the administrators individually cannot influence the global state of the blockchain. Their involvement is of a passive nature. They provide technical support to the functioning of the blockchain. They blindly execute the protocols of the blockchain.

(bb) How does it map to the GDPR?

29 A user sends data to the blockchain that are then further processed within the blockchain. The user instigates the initial sending of the data and is therewith controller of this initial transmission.[23] An interesting question is whether there are circumstances under which the GDPR considers the user (A in the example above) also as the controller of processing that occurs subsequent to transmission, i.e. when the data are with the administrators? The strongest argument for the user as a controller is that he chooses to use a certain blockchain or blockchain application. Therewith he also chooses the processing of data that flows from his choice. This is in line with the conclusion of AG Bot in the Wirtschaftsakademie case. Bot indicates that a Facebook fan page administrator should be seen as a controller, because he makes the processing possible by creating and operating the fan page,[24] even though he may foremost be seen as a user of Facebook.[25] It is also in line with the guidance document of the French CNIL where it says: “les participants, qui ont un droit d’écriture sur la chaîne et qui décident de soumettre une donnée à la validation des mineurs peuvent être considérés comme responsables de traitement.”[26] The CNIL seems to have thought in this context primarily of a user acting in a commercial or professional capacity. An example may be a public notary performing a payment for a client. The CNIL shirks back from the implications controllership has for a private user. It states that a user acting in a private capacity falls under the household exception. It is however unclear whether a private person placing a transaction on a public blockchain can also shelter under the household exception.[27] The Bitcoin blockchain is a public blockchain and the personal data of a Bitcoin payment’s recipient (B’s pseudonym in the example) become available to anybody. A private user would thus become a controller after all.[28]

[23] Compare Case C40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* [2018] ECLI:EU:C:2018:1039. The Fashion ID case concerns a Facebook like-button on a webpage, causing data about visitors to the website to be sent to and further processed by Facebook, irrespective of whether the visitors pressed the button. The question was whether the manager of the webpage who placed the Like-button on the page, was a controller together with Facebook for the collection of the visitors’ data and their disclosure by transmission. The CJEU found the manager’s determination of means contingent on 1. his awareness of collection and disclosure of personal data to Facebook and 2. his decisive influence over collection and transmission which would not have occurred without the plug-in (C-40/17, paras 77-78). His purpose was commercial advantage (C-40/17, para 80).

[24] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, Opinion of AG Bot, [2018] ECLI:EU:C:2017:796, para 56.

[25] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, Opinion of AG Bot, [2018] ECLI:EU:C:2017:796, para 53.

[26] CNIL (n 23) 2.

[27] CNIL (n 23) 3. CNIL does not indicate whether this also holds if the personal data are placed on a public blockchain.

[28] According to the old Lindquist-ruling of the CJEU, decided

30 Even though much points in the direction of the user as controller, some doubt can be derived from the ruling of the EUCJ in the Wirtschaftsakademie case. Even though the court decided that the fan page administrator was a controller, it did not rely on the argument that AG Bot brought forward. The court rather made the argument that a fan page administrator defines the parameters for the data processing and therewith influences the processing of the data itself.[29] That is much less the case with Bitcoin transactions. Bar a few small things (conditional payments), the blockchain protocol determines the parameters for Bitcoin payments. For other blockchain applications, such would need to be assessed on a case-by-case basis.

31 Where proponents of blockchain tend to present the blockchain as an environment in which users interact directly with each other, without reliance on intermediaries, the GDPR will not look away from the administrators of full nodes. They are likely seen as data processors (see section III.2) or even joint controllers (see below).

(cc) How to assess its mapping to the GDPR?

32 Assuming that the user is either individually or jointly a controller, is he able to fulfil his responsibilities as a controller? For fulfilling his responsibility, the user is dependent on the administrators of full nodes who perform the actual processing. The user as a data controller needs to make binding contracts with the full nodes who act as data processors or arrive at an arrangement where they are joint controllers.[30] In practice, it is not very well possible to conclude contracts with full nodes, because in a permissionless blockchain, there are many administrators, their identities may be unknown, new administrators may join anytime, just as old nodes may leave. In practice, no contracts are concluded at all. Even if a contract would come about, it is not at all certain that the user as a controller can exercise the necessary control over the full nodes. They will for example most probably be unable to delete data from the blockchain, to fulfil a request based on the right to be forgotten. Such deletion would render their participation in the blockchain pointless, as was described in section B above.

33 In practice, the main instrument of the user/controller to exert influence is to vote with his feet: the user/controller can compare various blockchains and if they exhibit relevant privacy-differences, choose the blockchain that best suits his data protection needs. In practice, this may come down to a user/controller having to opt for a permissioned blockchain that does not rely on crypto-economic incentives alone.

b) The administrators of nodes collectively offer a service

(aa) What is the conceptualization?

34 The administrators of full nodes together offer a service, such as enabling payments with a cryptocurrency. It perceives the blockchain administrators as a collective middleman. This conceptualization does not sit well with how proponents of blockchains usually portray them. The nodes forming the network in a permissionless blockchain never agreed amongst each other to form a network offering such service. Nodes can join or leave a permissionless blockchain at will. The coordination of their actions rests on a system of crypto-economic incentives, not on an agreement. The participation of nodes is motivated by their self-interest and they are indifferent to the result their participation gives rise to. Nevertheless, the conceptualization is worth exploring. Even though proponents of blockchains do not see the collective administrators as an intermediary, they do see the blockchain as a substitute for a traditional intermediary, such as a bank. Not seeing the collective administrators as a middleman, is to a large extent a form of framing to sell the idea that the blockchain is a technology that makes trust in middlemen superfluous.

(bb) How does it map to the GDPR?

35 Can the administrators of full nodes be joint controllers as meant in art. 26(1) GDPR? Thereto, it is required that two or more controllers jointly determine the purposes and means of processing. The CJEU ruled in the Wirtschaftsakademie case

under directive 95/46/EC, an internet publication falls outside the household exception (source: Case C-101/01 *Sweden v Bodil Lindqvist* [2003] ECR 1-12971, para 47). See also Vonne Laan 'Privacy en blockchain: wanneer is er voor wie privacywerk aan de winkel?' (2018) (1)(4) Tijdschrift voor Internetrecht section 3.2. Recital 18 GDPR seems to draw the boundaries of the household exception wider: "Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities."

[29] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, [2018] ECLI:EU:C:2018:388, para 36.

[30] Art. 28 lid 3 GDPR.

that a Facebook fan page administrator "by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities", contributed its part in setting means and purpose.[31] In the context of a permissionless blockchain, the full nodes cannot individually set the parameters of the core implementation, but together they can strongly influence the way the blockchain processes data. Core developers who can change the software are dependent on the administrators to adopt updated software. Without the administrators' adoption a change in the software will have no material effect. That is a strong argument for the administrators' controllership, in fact their joint controllership.

36 In the literature it has been argued that full nodes do not jointly determine purpose and means, because they do not conclude an agreement with each other:[32] a new administrator does not accede to an agreement, but he enters in a system ruled by crypto-economic incentives and involving certain data processing that he understands. Could the lack of a pre-existing agreement bar the finding of a "joint determination"? The GDPR does not require in so many words an agreement for finding a joint determination of purposes and means.[33] AG Bot in his conclusion in the Wirtschaftsakademie case stated that controllership is a functional concept. It is more about where the factual influence lies and relies much less on a formal analysis.[34] This underlines that even if there would be a contract, that the contract is not automatically determinative for controllership.[35] The argument that the administrators of nodes never agree amongst each other is thus not determinative under the GDPR.

37 Obviously, once parties have been found to be joint controllers, they need to determine their respective responsibilities by means of an arrangement.[36] That is however the legal consequence of being joint controllers, rather than a requirement for finding joint controllership in the first place.

38 The administrators of full nodes will usually not have actual knowledge of the personal data their computer systems process. Theoretically, they could know since permissionless blockchains are always public, but the volumes of data are usually too big for an administrator to obtain actual knowledge. Nevertheless, their lack of actual knowledge is not an objection against a finding of joint controllership. The CJEU decided in the Google Spain case, that a search engine can be a controller even though it does not have control over the personal data third parties publish on their websites.[37] In the Jehovan case, the CJEU decided that joint controllership does not require that each controller has access to the personal data.[38]

39 In the STOA report of 2019, it is remarked that the GDPR rules about joint controllership are unclear.[39] Each joint controller is fully responsible towards data subjects, but at the same time it is observed that there may be controllers amongst the "joint controllers" that are factually unable to take the measures that are needed to discharge themselves

[31] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, [2018] ECLI:EU:C:2018:388, para 39.

[32] Rainer Böhme and Paulina Pesch, 'Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie' [2017] DuD 473, 479.

[33] Art. 26(1) GDPR. Finck (n 1) 100, however seems to see an arrangement as a condition for joint controllership.

[34] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, Opinion of AG Bot, [2018] ECLI:EU:C:2017:796, para 46.

[35] This is in line with how the art. 29 WP approaches the term 'determine' (admittedly in the context of a single controller) in Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010, 8. In the same vein also Christian Wirth and Michael 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> accessed 21 October 2019, 5 and R Mahieu, J van Hoboken and H. Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe', (2019) 10 Jipitec 39, 44, para 21. CNIL does not directly address this issue: "Lorsqu'un groupe de participants décide de mettre en oeuvre un traitement ayant une finalité commune, […] tous les participants pourraient être considérés comme ayant une responsabilité conjointe, conformément à l'article 26 du RGPD […]." CNIL (n 23) 3.

[36] Art. 26(1) GDPR.

[37] Case C131/12 *Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Maria Costeja Gonzalez* [2014] ECLI:EU:C:2014:317, 34.

[38] Case C-25/17, *Tietosuojavaltuutettu and Jehovan todistajat — uskonnollinen yhdyskunta* [2018] ECLI:EU:C:2018:551, 69.

[39] European Parliament, 'Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?' (STOA) 54-55, <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf > accessed 25 May 2020.

of their responsibility. In my view that is not so much an issue of lack of clarity. The GDPR leaves it rather to the parties (the joint controllers) to resolve this. The controllers who are not able to take the measures themselves, must make sure there is an arrangement in place that allows them to require other controllers to take the necessary measures. That this is hard to achieve in the context of permissionless blockchains in their current form is something else and does not necessarily mean that rules need to be relaxed for systems that do not very well allow responsibility to be attributed.

(cc) How to assess the mapping to the GDPR?

40 To exercise certain responsibilities (such as the duty to correct data, to erase data or certain transparency obligations) the administrators within the blockchain need to cooperate with each other. However, the blockchain coordinates only a (payment) transaction service, and there are no crypto-economic incentives to coordinate compliance with the GDPR. Theoretically, somebody may devise a crypto-economic system of incentives to comply with the GDPR. However, for the time being it is unclear how such system could be made.

41 The only practical way for nodes to realise joint control is to ensure that the nodes arrive at an arrangement in the form of a traditional agreement amongst each other. The current practice is not that nodes in a permissionless blockchain make an agreement.

42 If they would, this brings compliance with the GDPR much closer. Data subjects would know whom to address. Additional technical and organisational measures in the context of security, privacy-by-design and privacy-by-default could be realised. The administrators of nodes would collectively be able to influence what personal data for what purposes would be collected and processed. The nodes together would be a strong countervailing force against the core developers. However not all problems may prove solvable, such as deletion of old data from the blockchain.[40] That is something that cannot be solved by placing controllership with another party. However an agreement would be part of a nascent governance structure for a blockchain. A further developed governance structure may be able to resolve issues that go beyond merely fulfilling the duties of a controller and allow a blockchain to adapt to any changing circumstances in the environment in which it functions.

c) Each full node is an individual controller only for his own processing operations

(aa) What is the conceptualization?

43 In this conceptualization, the administrator of a full node provides an individual service, for example consisting in verification of transactions. This conceptualization strongly builds on the idea that no contracts exist between administrators of nodes. Each node is an individual entrepreneur who participates in the blockchain and adheres to its protocol strictly from a well-understood self-interest. The activities of full nodes are purely coordinated via the core code of the blockchain and the incentives it creates. This is a technical and economic orchestration.

(bb) How does the conceptualisation map to the GDPR?

44 Each administrator is only a controller for the processing of personal data he performs.[41] He determines purpose and means by choosing which blockchain to participate in. An administrator has two roles: on the one hand the role of full node, on the other hand the role of miner (in Bitcoin and Ethereum 1.0) or validator (in Ethereum 2.0). The roles can also be divided over separate actors. The task of the full node is to check whether transactions conform to the protocol and to store a copy of the blockchain. His purpose is to select or reject transactions for inclusion in a block and the means is a check of a transaction against data present in the blockchain. His activity is directly involved with the

[40] There are academic explorations seeking to create a permissionless blockchain from which data can be deleted. For example: Martin Florian, Sophie Beaucamp, Sebastian Henningsen, Björn Scheuermann 'Erasing Data from Blockchain Nodes' 2019 Humboldt Universität zu Berlin / Weizenbaum Institute. <https://arxiv.org/pdf/1904.08901.pdf> accessed 22 October 2019. They present a system that allows some nodes to erase data as long as there are other nodes that maintain the entire chain. Another example: Dominic Deuber, Bernardo Magri and Sri Aravinda Krishnan Thyagarajan 'Redactable Blockchain in the Permissionless Setting' December 4, 2018 <https://bernardomagri.eu/wp-content/uploads/2018/12/redactable_premissionless.pdf> accessed 22 October 2019. They developed a system in which administrators can vote about deletions. These solutions are theoretical and have not been proven in practice.

[41] Luis-Daniel Ibáñez, Kieron O'Hara, and Elena Simperl, *On Blockchains and the General Data Protection Regulation* (University of Southampton 2018) pt 3, 4. Laan (n 29) classifies this as differentiated controllership.

personal data in a transaction and has a function that is relevant in society (prevention of double spending for example). The task of the miner or validator is to contribute to a decision about what block to include in the canonical blockchain and make sure the versions or copies of the blockchain stay in sync with each other. This is a more technical task and its first focus is a block, not an individual transaction or the personal data contained therein. This also makes it difficult to formulate what the purpose of a miner or validator in relation to the personal data is. A miner is not a controller. In this light, it can be understood that a miner is often compared with an administrator of an email server.[42] Such an administrator is not a controller of the personal data contained in the body of an e-mail message.[43] What holds for the miner, also holds for the validator. He performs the same function. That a validator does not perform calculations is not relevant. A miner is a controller because of the role he fulfils. The precise activities (calculations) are not so relevant, rather the function the activities play. That said, it must be borne in mind that the term validator is somewhat misleading because it might suggest that in Ethereum 2.0 no distinction is made between a validator and a full node.

(cc) How to assess the mapping to the GDPR?

45 For the data subject exercising his rights, it is of little interest to obtain the cooperation of a single node. Unlike the WWW, where it may be useful to have one's personal data removed from a website – even though the same data may be present on another website – exercising one's rights affecting one copy or version of the blockchain has markedly less effect. The different copies or versions of a blockchain stand in much closer rapport. The versions are compared frequently to know which versions represent the valid chain. Exercising one's rights vis-à-vis one version has no effect if other versions remain unaffected. Moreover, removing data from a version of the blockchain almost certainly disqualifies this version from meaningful participation in the blockchain.

46 A data subject exercising his rights needs coordination within the blockchain, so that effect is given to his rights in many or even all versions of the blockchain. As we have seen above, a permissionless blockchain does not support such coordination. In fact, with each administrator of a full node being a separate controller for only his own data processing, the task (and cost) of coordination is shifted to the data subject. He would need to address many individual nodes separately. This makes it practically impossible for the data subject to exercise his rights. In other words, the cost of the coordination problem, is laid at the doorstep of the data subject. In terms of the GDPR, the data processing is not transparent for the data subject.[44]

d) The core developers

47 Could the core developers be seen as joint controllers together with the actor(s) that have above been identified as potential controllers? The core developers write the code that when run by nodes constitutes the blockchain and its native crypto-currency. As code-writers they initially set many parameters. For example they code how a user performing a payment with the crypto-currency authenticates him or herself. They also set the purpose initially. For example, they build a system for payments with a crypto-currency or an ICO. However, code alone is not a blockchain. It only becomes a blockchain if administrators decide to adopt the code. For decisions on the development of the code, a governance structure is usually in place. Even though the core-developers surely have a say, the goal of the governance structure is usually to give other stakeholders, such as the administrators, influence as well. Furthermore, actual personal data do not flow through the computer systems of the core-developers. They only provide the technology. That does not necessarily mean that they cannot be a joint-controller. In the Jehovah case, the CJEU decided that not every joint controller needs to have access to the personal data.[45] Hence, the law does not preclude that core developers are joint-controllers. However, a strong argument to see these technology providers as controllers does not exist either.

[42] M. Martini & Q. Weinzierl, 'Die Blockchain-Technologie und das Recht auf Vergessenwerden' [2017] Neue Zeitschrift für Verwaltungsrecht 1251, section II(2)(a). Also European Union blockchain observatory and forum, *Blockchain and the GDPR*, 2018, 18. European Parliament (n 40) 46 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 5 May 2020.

[43] Recital 47 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[44] Laan (n 29) pt 3.3.

[45] Case C-25/17, *Tietosuojavaltuutettu and Jehovan todistajat — uskonnollinen yhdyskunta* [2018] ECLI:EU:C:2018:551, 69.

III. The processor of personal data

48 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(8) GDPR). For an actor to be a processor, it needs to be on the one hand a “separate legal entity with respect to the controller and on the other hand processing personal data on his behalf”.[46]

49 In a permissionless blockchain where an application is embedded in the core code, it depends on the factual relationship between a full node and a miner whether the latter can be said to act on behalf of the former. Full node and miner may even be roles that are united in one entity (in which case the miner obviously is not a processor), but it may also be separate entities that have tighter or closer relations towards each other. The qualification of a miner as processor would then come to depend on the peculiarities of the individual case. Could a miner be a processor acting on behalf of a user/controller?[47] This appears to be rather unlikely. Users do not know the miners and do not have contractual relations with them.

D. Conclusion

50 Who is or are the controller(s) in permissionless blockchains? This article has approached this question by asking where to place the prime responsibility: with the user, with the administrators of full nodes collectively or with the administrators of full nodes individually? In the Wirtschaftsakademie case and Fashion ID case, the CJEU took a broad approach in order ensure complete and effective protection of the data subject.[48] When examining who sets purposes and means of data processing, the court took a functional approach, asking who set(s) the parameters for the data processing.

51 Turning to our case of a permissionless blockchain and the three conceptualizations of the relations between actors in a permissionless blockchain, the following picture emerges.

52 First, could the user be a controller? Where the user does not place the code of a smart contract on the blockchain (but for example uses an application embedded in the core code), the user has only limited possibilities to set the parameters of data processing. Nonetheless, it can be desirable to designate the user who is a professional party as a joint controller together with the administrators, because it creates a clear addressing point for a data subject seeking to exercise his or her rights. Especially from the perspective that the choice of controller(s) should ensure a complete and effective protection, this approach is beneficial.

53 Seeing the administrators of full nodes as individual controllers strictly for their own data processing on their servers sits well with the way in which proponents of blockchains see them: downplaying the role of administrators as individual actors that have little influence on the blockchain overall. From a GDPR perspective this is not acceptable. Complete and effective protection of the data subject requires coordination within the blockchain. In this conceptualization, the problem of achieving coordination is completely laid at the doorstep of the data subject. He needs to approach sufficiently many administrators to get the global state of the blockchain changed, if he or she succeeds at all. This does not give complete and effective protection.

54 Seeing the administrators as joint controllers together with the core developers is the strongest argument. They have the largest influence on the data processing that takes place. Currently, a joint controllership of administrators in a permissionless blockchain may not function very well. De facto administrators may be individual entrepreneurs that do not conclude an arrangement amongst each other as required by art. 26 GDPR. However, it is questionable whether that is a situation that will last. In the end, a blockchain is a living phenomenon that adapts and grows with changing needs. From a broader governance perspective, administrators will want to have influence on the further development of their blockchain and not leave it completely to a select group of core developers. The practical demands on a system that has to function in a changing environment will drive administrators to collective arrangements on the governance of their blockchain. This lays the basis for joint controller arrangements.

55 Those that see blockchain as the ultimate means to make intermediaries superfluous, might have preferred the view that no controller at all could

[46] Art. 29 WP, Opinion 1/2010 on the concepts of “controller” and “processor”, WP 169, 25.

[47] This is also relevant in cases where the application for which personal data are processed is a user-defined smart contract.

[48] Concept of complete and effective protection mentioned in Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, [2018] ECLI:EU:C:2018:388, para 28 and in Case EUCJ, 29 July 2019, C40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* [2018] ECLI:EU:C:2018:1039, para 66.

be identified. That is however a possibility that the law seeks to prevent. The CJEU defines the concept broadly to ensure effective and complete protection of the data subject.[49] It is indeed difficult to imagine how data protection could be realized without any actor having to take responsibility and for the data subject no address to turn to when exercising his or her rights.

[49] Case EUCJ, 29 July 2019, C40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* [2018] ECLI:EU:C:2018:1039, paras 65, 66 & 70. Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, [2018] ECLI:EU:C:2018:388, paras 26-28 & 42.