Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data

Conference Paper · May 2018

DOI: 10.18420/blockchain2018_03

CITATIONS
79

READS
942

2 authors:

Michael Kolain
Deutsches Forschungsinstitut für öffentliche Verwaltung Speyer
12 PUBLICATIONS **93** CITATIONS
SEE PROFILE

Christian Wirth
Privacy by Blockchain Design
3 PUBLICATIONS **79** CITATIONS
SEE PROFILE

Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data

Christian Wirth
Senior Blockchain Architect (IBM)
Freie Universität Berlin
wirth@protectivecircle.com

Michael Kolain
Research Associate (Law)
German Institute for Public Administration
Speyer
michael.kolain@posteo.de

ABSTRACT

This paper takes an initial step forward in bringing to life the certification mechanisms according to Art. 42 of the General Data Protection Regulation (GDPR). These newly established methods of legal specification act not only as a central vehicle for overcoming widely articulated and discussed legal challenges, but also as a sandbox for the much needed close collaboration between computer sciences and legal studies. In order to illustrate, for example, what data protection seals could look like in the future, the authors propose a methodology for "translating" legal requirements into technical guidelines: architectural blueprints designed using legal requirements. The purpose of these blueprints is to show developers how their solutions might comply with the principle of Privacy by Design (Art. 25 GDPR). To demonstrate this methodology, the authors propose an architectural blueprint that embodies the legal concept of the data subject's consent (Art. 6 sec. 1 lit. a GDPR) and elevates best practice to a high standard of Privacy by Design. Finally, the authors highlight further legal problems concerning blockchain technology under the GDPR that will have to be addressed in order to achieve a comprehensive certification mechanism for Privacy by Blockchain Design in the future.

ACM Classification Keywords

10002978.10003029.10011150 Security and privacy: Privacy protections

Author Keywords

Blockchain; Privacy by Design; GDPR; Personal Data; Smart Contract; Data Protection

INTRODUCTION

Handling Personal Data in the digital world and the opportunities of blockchain technology

The more digitalized our every day life becomes, the more important it is from a privacy perspective to have control over the data we emit. According to the GDPR, the procession of personal data by any party requires either the consent of the data subject or a legal basis (Art. 6 GDPR). However, today's IT-systems are not capable of providing this functionality in an ideal sense. Rather, the status quo remains as follows: Personal data is purported to be stored according to legally binding security standards in company-owned or cloud-based data silos, without mutual confirmation between data subject and recipient that this information is being handled responsibly.

The consent of the data subject is the central vehicle for ensuring everyone's right to the protection of personal data (Art. 16 section 1 of the Treaty on the Functioning of the European Union, TFEU). Consent links the processing of personal data to the free decision of the data subject–in an ideal sense for both initial and subsequent processing. However, under the architecture currently in use, the data subject must have confidence that the recipient of the consent processes his personal data lawfully and that the data protection authorities otherwise perform their supervisory function responsibly. However, given today's methods of storing and accessing data, the individual usually cannot directly retrace what happens to his personal information in the IT-system of the controller. As a result, the individual is mostly limited to giving his or her consent beforehand, in a way that is based on an abstract clause (e.g. "... for purposes of health improvement") rather than on a more transparent case-by-case basis.

Although the supervising bodies of the EU member states monitor the data market and can sanction infringements, they underlie the same restrictions as the data subject in order to detect a unlawful subsequent processing not covered by consent. Until now, their ability to guarantee a 'consistent and high level of protection of natural persons' (Recital 10 GDPR) has been severely limited–one of the main reasons being the technical status quo just described.

Despite widespread concern about the safety of the digital sphere, the Web 3.0 [8], in combination with blockchain-technology and modern cryptography, can bring personal data management to a level of privacy and security that prioritizes individual sovereignty and shared transparency. The semantic web gives meaning to data in the digital space, allowing it to be classified and encrypted accordingly. The blockchain can then act as a tamper-proof ledger to record digital interactions; the data subject can verify where his personal data is stored and put to (commercial) use. Today, data is present

Wirth, Christian; Kolain, Michael (2018): Privacy by BlockChain Design: A Blockcchain-enabled GDPR-compliant Approach for Handling Personal Data. In: W. Prinz & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies

ISNN 2510-2591.

DOI: http://dx.doi.org/10.18420/blockchain2018_03

in vast multiplicity, with each copy representing the state of this data at the point in time when it was saved. The Web 3.0 allows us look at this from a new perspective: Instead of saving copies of the relevant data, which could potentially become outdated from the second it is stored, users should keep pointers to the origin of the data, which they know will always provide the most up-to-date version of the information. In addition, smart contracts can now be executed completely automatically on behalf of digital identities, which enables us to provide personal data to a third party whenever access to it is required. Third parties can file a request for access, and a smart contract will check the validity of this request and handle it accordingly–transparently for all parties involved.

For a GDPR-compliant blockchain solution predefined by the specific requirements of a certification mechanism, giving and withdrawing consent will form a necessary base element. In the experiment documented by this paper, the goal was to determine what architecture we would end up with if we used the law as the base requirement for designing a minimal, sufficient architectural blueprint representing the legal concept of the data subject's consent. In order to allow the reader to follow our interdisciplinary journey we will first present the concept of Privacy by Design according to the GDPR and explain our methodology of architectural blueprints. Next, to demonstrate our methodological approach, we will introduce our own blueprint focusing on the data subject's consent in a blockchain-enabled and GDPR-compliant manner. We will then outline further legal challenges that could not be covered in this paper, but will play a crucial part in the further development of certification mechanisms in accordance to the GDPR. We will conclude with some general thoughts on why blockchain is an important technology enabling us to rethink obsolete design models and establish new standards for trust, transparency and privacy under which personal data could be handled in the future.

PRIVACY BY DESIGN UNDER THE GDPR AND CERTIFICATION MECHANISMS

The GDPR came into effect within all member states of the European Union on May 25th, 2018. One of the major requirements when it comes to handling personal data is that the underlying IT-systems follow the concept of **Privacy by Design** (Art. 25 GDPR). In its most basic sense, it asserts that "privacy should be promoted as a default setting of every new IT system and should be built into systems from the design stage" [7]. In the more complex words of Art 25 sect. 1 GDPR, it obliges the controller to implement "appropriate technical and organisational measures (...) which are designed to implement data-protection principles (...) in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". As a simple example, one consequence would be that personal data must not be stored in plaintext on blockchains.

While these legal requirements remain highly abstract and, thus, open to interpretation, Art. 25 sect. 3 GDPR leaves room for specifications: "*Approved certification mechanisms* pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements." The concept of EU-wide certification mechanisms is new to EU data protection law. Their purpose is "to enhance transparency and compliance with this Regulation" and allow "data subjects to quickly assess the level of data protection of relevant products and services" (Recital 100 GDPR). Especially for new technologies, like blockchain, which occupy the margins of the GDPR's legal doctrines, the process of certification–which includes **data protection seals and marks**–can serve as a means for legal certainty, as it fulfills the "purpose of demonstrating compliance with this Regulation" (Art. 42 sec. 1 GDPR).

However, being certified does not guarantee, but rather only indicates, the legal processing of data. What's more, it will not be mandatory for software to be certified. Still, the certification mechanisms bear the potential–even as a "voluntary" (Art. 42 sec. 3) measure–to set standards, thereby boosting technological advancement in the market. It is therefore foreseeable that certification mechanisms will play a crucial and practical role in defining compliant ways of processing personal data under the GDPR [2]. It is likely that the supervisory bodies and the newly established European Data Protection Board (Art. 68 ff. GDPR) will take steps in this direction fairly soon–and they will need scientific help from the blockchain community. In order to master the herculean task of defining technology-specific standards, the fields of computer science and law must align themselves more closely–a perspective that supplies the impetus for our interdisciplinary work [10] and [11].

METHODOLOGY: ARCHITECTURAL BLUEPRINTS AS AN ELEMENT OF CERTIFICATION MECHANISMS

The architectural blueprint introduced in the following section tries to give a first methodological answer to how the certification mechanisms of the GDPR could narrow down specific standards. As there are no particular specifications in Art. 25 GDPR for how privacy by design should work or which properties a system inspired by or built on blockchain-technology should have, this paper aims to provide a general approach for architectural system designs.

Rather than propose an entire framework for a certification mechanism (which would go widely beyond the limits of this paper), we attempt to integrate a single legal requirement into a blockchain-enabled-architecture that builds upon the ideas of Privacy by Design.

As a central vehicle to protect personal information in the digital world (see Introcution), **the data subject's consent** (Art. 6 sec. 1 lit. a GDPR) seems like a good starting point. This is so because, firstly, the legal outlines of the consent have already undergone a thorough academic and practical discourse. This makes it relatively simple to model consent in a distributed architecture in contrast to other more controversial legal requirements, such as an implementation of the Right to Erasure. Secondly, consent forms a fundamental legal category in order to justify the processing of personal data under EU legislation. Therefore, future data protection certificates, seals and marks will have to cover this aspect as a base element.

Our technical proposal, however, does not stop with defining solely minimal standards for implementing the concept of consent into an IT-solution. It rather aims to contribute to a (potential) data protection seal that marks a high standard of Privacy by Design. By doing so, we also want to propose a new generation of systems handling personal data. Consequently, we utilize an architectural blueprint that both guarantees compliance with the GDPR concerning consent and sets new standards that embrace the core ideas nurturing the concept of Privacy by Design.

TECHNICAL DETAILS

First we start with the "translation" from the legal requirements about consent to technical requirements.

Broken down to the technical level, consent means that the data subject, first, **shall be asked once for approval** when someone wants to process his or her personal data and, second, has to be able to **withdraw their consent** given to a specific party (Art. 7 sect. 3 GDPR).

In addition to the minimal requirements to be GDPR-compliant mentioned above, the solution supports and reflects that data subjects should be given control over and allowed to reclaim their personal data as they see fit. Therefore data subjects are **notified whenever their personal data is processed**; changes to access rights are instantaneously reflected on the endpoint providing the personal data to the controller.

To make a distinction from personal data in a legal sense, the technical representation of it shall be called *Set of Personal Data (SoPD)*.

Actors of the Use Case

- **Issuing Party**: the entity guaranteeing that a particular SoPD is authentic
- **Data Subject**: the person to whom a SoPD relates to
- **Third Party**: the party requesting a SoPD

Explanation of Cryptographic Expressions:

- $*R$ Denotes a pointer to a resource R
- $H(X)$: The hash of a SoPD X
- $Enc()$: The function of an encryption scheme used to encrypt the SoPD in plain text using the public key of the data subject
- $Dec()$: The function of an decryption scheme used to decrypt the SoPD in cyphertext using the private key of the data subject
- $Enc(P)$: The resulting Cyphertext using $Enc()$ on the SoPD P in plaintext
- $Dec(C)$: The resulting Plaintext using $Dec()$ on the SoPD C in cyphertext

The data subject is the only person who should be able to decrypt the SoPD; therefore we use a suitable asynchronous-public key encryption scheme, where the issuing party encrypts the verified SoPD using the public key of the data subject, sends the $Enc(SoPD)$ to the data subject, and keeps only the Hash of the Set of Personal Data $H(SoPD)$.

Issuing Party

The **issuing party** stores a set of the following information on their blockchain or blockchain-compatible data storage:

- $H(SoPD)$: The Hash of the SoPD
- $*SC(SoPD)$: A pointer to the access-point of a smart contract to request the required SoPD

The Hash of the SoPD is stored on a blockchain-compatible data store of the issuing party in order to allow any third party to check the validity of the decrypted SoPD that has been delivered directly by the data subject's smart contract. The pointer reveals the access point to a smart contract handling every request for a SoPD. This ensures that the data subject is notified every time his or her data is requested in order to be processed. From the perspective of the self-determination about one's personal data, this is an ideal situation: The data subject can give specific consent case-by-case (or inspect if the smart contract was applied correctly in each case) rather than having to declare his or her consent beforehand in an abstract way without being able to control each processing. In contrast, from the perspective of a company working with personal data, this could lead to a higher administrative burden.

Data Subject

The **data subject** provides a smart contract, allowing third parties to request a subset of or a full SoPD. This service allows the data subject to decide on how to react to requests – and which subsets of personal data he or she wants to share. The following Figure 1 shows the connection flow and the underlying interaction between the smart contract provided by the data subject, the third- and the issuing party. The interaction parts for the third party requesting the SoPD will be described in the next subsection.

Smart Contract

The smart contract handles only a single type of SoPD by one issuing party to be provided to third parties. The third party initializes contact to the smart contract once, requesting a certificate for future access to the SoPD. Given that the data subject gives his consent to the recipient's request (and does so "freely" as demanded by Recital 11 GDPR), an up-to-date SoPD can from now on be requested just in time, when it is needed for processing. The smart contract will provide the SoPD immediately as long as the certificate of the third party is valid. There is now no more need to store the actual personal data for the third party.

The smart contract has to meet the following minimal requirements:

- The smart contract has an interface that can handle the initial request of a certificate for future requests of an SoPD.
- The smart contract has access to a securely hosted decryption function, which will provide the function $Dec(X) = Enc(SoPD)^{-1}$.

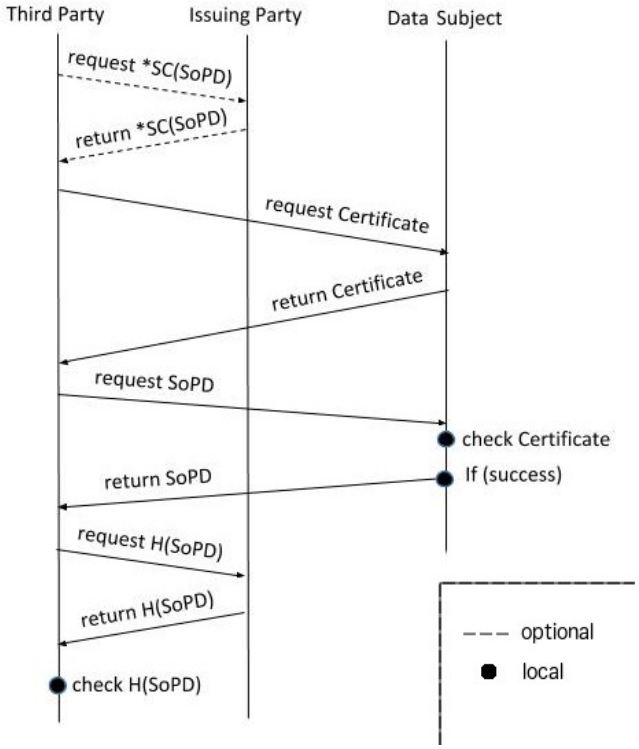

Figure 1. Flow diagram of communication between data subject, issuing party and third party

The critical part here is the key used for decryption, as security stands and falls with the secrecy of this private key [6]. In order to ensure that the data subject is notified whenever a SoPD is accessed, it would be required that the data subject is the **single source**, providing the smart contract capable of decrypting the SoPD in question. In favor of practicality, this functionality can be handled by a blockchain functioning as an immutable access-log as Zyskind and Nathan have shown in their paper [12].

The following model describes a minimal interface for a smart contract that allows a third party to request a SoPD ensuring that the data subject is always notified whenever one of his SoPD is disclosed to any third party:

- RequestCertificate(ThirdPartyID, ReasonForRequest)
- RequestSoPD(Certificate, RequestedSubsetOfSoPD)
- Access to Oracle for $Dec(X)$, where X is element of $Enc(SoPD)$
- CheckValidityOfCertificate(Certificate) Checks if the requesting party is allowed to be given access to the SoPD based on the certificate provided with the request.

It would be unrealistic to expect a service provided by the data subject to be highly available, or to assume the average user is capable or willing to set up such a service and maintain it. However, this is where blochckain comes into play: it is the missing puzzle piece in achieving high availability while maintaining full control over one's personal data. Zyskind et al. have shown that an architecture using blockchain can solve this problem quite elegantly [12].

In addition, there are no guarantees that copies of this SoPD are still up-to-date as soon as the hash of the SoPD $H(SoPD)$ has changed. This can easily be achieved by modifying a timestamp in the SoPD whenever it is requested, as changing only the timestamp without touching the relevant personal data results in another hash, and forces third parties to file a new request against the smart contract provided by the data subject if they want to make sure that they process an up-to-date SoPD. This would also allow them to identify any processing of an outdated SoPD by the third party without requesting it for just-in-time processing. Through this mechanism it is possible to identify third parties that store personal data without the data subject's consent. Changing the hash $H(SoPD)$ in combination with invalidating the third party's certificate also can serve as a tool to withdraw a once given consent (Art. 7 sect. 3 GDPR).

For security reasons, a separate key pair is to be generated for every smart contract. This allows us to invalidate the public key in case the private key for this particular SoPD is compromised. It also minimizes the effort to mitigate the damage as only the SoPD encrypted with the compromised key has to be encrypted with a newly generated keypair.

For efficiency reasons, the service of the data subject could also provide a smart contract informing a third party if a previous request of a SoPD is still up-to-date. This would not conflict with the requirement of every request to notify the data subject, as each inquiry is linked to the recipient by the Certificate.

FURTHER LEGAL CHALLENGES CONCERNING BLOCKCHAIN TECHNOLOGY

While the terminological foundation of the GDPR is only hardly compatible with decentralized database structures like Distributed Ledger Technology (blockchain in particular), it also comes with many innovations [9]. Still, legal uncertainty is one of the main obstacles for a widespread adoption of blockchain solutions, especially in the common market of the EU. A closer look at data protection law can, however, show a way out of the legal deadlock. The academic debate could lead into additional architectural blueprints which can be used in the certification processes ensuring Privacy by Design under the GDPR.

Personal Data

First of all, the scope of the GDPR applies only if **personal data** (Art. 4 sect. 1 GDPR) is involved. At first glance, a blockchain handles no names, addresses, or e-mail IDs - only hashes and encryption keys. Therefore, especially in the non-legal debate, blockchain-data is often referred to as "anonymous" - and since anonymous data is not subject to the GDPR [1], blockchain could thus per se fall out of the scope of

[1] According to Recital 26 GDPR information is anonymous if it "does not relate to an identified or identifiable natural person" or if "personal data is rendered anonymous in such a manner that the data subject is not or no longer identifiable"

data protection law and its regulatory corset. However, this is too simplistic. In many cases, there will be an entity that can identify the person behind a private key - e. g. when the data subject is buying an item using a cryptocurrency (and leaves his address for delivery) or for someone using methods such as Chainanalysis to mine the data in a public blockchain making sense out of the usage of a specific private key. Therefore, many use cases of blockchain are not anonymous [3]; rather, they are - in the legal sense - examples of *pseudonymity*. This is the case if personal data "can no longer be attributed to a specific data subject without the use of additional information" (Recital 26 GDPR). In other words: data is pseudonymous if someone has the possibility to combine it with other available information and can thus identify a person; and it is anonymous if this possibility does not exist. Since means of pseudonymity are still "personal data", the scope of the GDPR will still apply for a wide range of blockchain-solutions.

However, blockchain-data could, theoretically, fall through the cracks of data protection law if the person behind the data cannot be identified directly or indirectly by a person trying to do so. Data is considered anonymous if the identification of a person - even if theoretically possible - would need disproportionatly high measures, taking into account "all the means reasonably likely to be used," including "all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments" (Recital 26 GDPR). In a legal sense, the GDPR would not be applicable in such a scenario of anonymity. However, the "means likely to be used" and "available technology" come with legal uncertainty for IT-architects. What could be considered anonymous data today, could be personal data in five years or some entities could have a high computing power available to attack the encryption while others don't. Furthermore, as many blockchain-applications will operate in use-case scenarios that make it necessary to identify a specific person, true anonymity would not be a feasible design-decision there anyway.

From the standpoint of Privacy by Design, we propose as a groundrule: the more difficult an IT-system renders the option to identify a person behind blockchain-data and the closer it comes to anonymity, the more compliant it is with the virtues of the GDPR. We therefore suggest to develop a design that clearly appoints certain actors to be able to point (pseudonymous) blockchain-data to a specific person by using additional information while keeping the dataset as unidentifiable as possible for other actors.

Controller

Apart from many innovative rules that aim to update the law of data protection from the old Directive 95/46/EC to a legal framework that reacts to "rapid technological developments and globalisation" (Recital 8 GDPR), the legal doctrine forming the foundation of the GDPR still reflects a limited technological understanding–at least when it comes to methods of decentralized and distributed IT-systems. The GDPR bears in mind administrators but not Peer-2-Peer-networks. By addressing mainly the **controller** as the target of the duties of the GDPR–defining him as "the natural or legal person (...) which, (...) determines the purposes and means of the processing of personal data" (Art. 4 subsection 7)–the regulation focuses mainly on entities which have the ability to actively control the data-flow of an IT-system. Blockchain-technology breaks with this understanding. While, in permissioned blockchains, the entity who manages the key infrastructure potentially also determines the purpose and means to a certain degree that will in most cases make them the controller, in permissionless blockchains there is no obvious controller: the miners have an economical interest in the transaction but are not concerned with the (personal) content of the distributed ledgers, and the programmers lose their influence after the blockchain is set into motion. As a result, only each individual node is, legally, in control [9].

However, the (new) category of **joint controllers** in Art. 26 GDPR may apply, if the nodes "jointly determine the purposes and means of processing." The provision opens a way to represent more complex computational relationships with equal responsibility–and it could even reach out to cover decentralized scenarios like blockchain technology. However, it is not yet clear whether the duty to transparently "determine their respective responsibilities" in an explicit arrangement (to make available for the data subject, Art. 26 sec. 2 GDPR) is the *cause* of joint controllership or rather its *consequence*. In case only those who explicitly agree to be joint controllers would fall under Art. 26 GDPR, there would be only but a small incentive to actually make use of the new category in blockchain scenarios. Determining whether or not to accept and share a legal responsibility would lie solely in the hands of the nodes of a decentralized network. Before this background, it seems rather likely that the law attempts to solidify objective requirements for joint controllership: the new category would then cover all (factual) situations of equal influences on the purposes and means of processing–and require them to make an arrangement. Every infringement of this duty in Art. 26 GDPR could lead to drastic sanctions (Art. 83 sec. 4 lit. a GDPR).

But the question of whether a blockchain-network is really a case of joint control remains hotly contested. Some voices in academia have argued against it, stating that the rules of a blockchain-network stem not "from an agreement of the nodes, but ultimately merely the sum of their independent behaviour" [4]. Whether a notion of *intention* to agree is necessary can surely be questioned, however. The fact that nodes have equal influence and freedom to choose (or start) a certain blockchain-network–and can, for example with the necessary majority or by a Fork, change the rules–rather argues the opposite. These points make a convincing case for the interpretation that blockchain-networks should be considered a subset of joint controllership (Art. 26 GDPR)–with the result that a transparent agreement about the responsibilities becomes the prerequisite for a compliant application (and otherwise sanctions may apply). Blockchain developers would therefore be forced to consider the liability side of data protection already in the design stage–another layer on top of (other) privacy questions. However, this could lead to a huge downfall for the adaption of blockchain-networks and hamper

the innovative potential of decentralization behind blockchain technology. It would lead to the questionable result, that a supervisory body could just pick any node of a (permissionless) blockchain-network and sanction them for the mutual behaviour with thousand other unknown users.

Since the academic and legal discussion about the question "who is the controller of a (permissionless) blockchain?" is still rather in its infancy, certification mechanisms could play a crucial role in narrowing down architectural decisions while other questions still remain unsolved.

Right to Erasure

Even if–with some effort of legal interpretation–personal data is concerned and a controller is found: How can a blockchain-based system implement the **data subject's rights**, such as "the obligation to erase personal data without undue delay" put forward in Art. 17 sect. 1 GDPR or even "take reasonable steps (...) to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data" (Art. 17 sec. 2 GDPR)? While in permissioned blockchain scenarios technical steps have been identified to erase data without interrupting the functionality of the blockchain [1], in permissionless blockchain scenarios such as Bitcoin, no single node is able to efficiently eliminate a set of personal data requested for erasure or inform the network about such a request [9]. It's one of the main challenges for blockchain developers to comply with "the right to be forgotten" in Art. 17 GDPR [5]. In an ideal scenario, the participants of a blockchain-network would agree on an effective process to (jointly) execute a lawful request to erase personal data from the decentralized ledgers.

INTERMEDIATE RESULT AND FUTURE WORK

A technical framework based on blockchain technology must find ways to cope with and implement the manifold legal requirements of the GDPR, while legislators are called upon to seek new forms of legal doctrine that stay abreast of technological changes–especially if they (like blockchain) bear the possibility of decreasing the dangers of uncontrolled, nontransparent, and often unlawful processing of sensitive personal data.

The certification mechanisms specifiying the Privacy by Design doctrine (Art. 25 sec. 3 GDPR) can serve as a tool to find a common way between legal requirements and technical design decisions. They can mark minimal requirements or high standards for GDPR-compliant IT-solutions. In future research, we will address additional aspects beyond the data subject's consent (as a central vehicle of self-determination) by "translating" legal requirements into architectural blueprints.

CONCLUSION

This paper has shown that architectural blueprints can serve as a methodological tool to translate legal into technical requirements in a comprehensible way. An architectural blueprint's main function is not to be implemented in a specific product, but rather to give a technical audience–those capable of creating software for production–an idea of a technical reflection of legal demands about IT-systems.

Even though blockchain was not the main component of the proposed architecture, we regard it as a cornerstone in enabling decentralized, trustworthy transactions between a multitude of pseudonymous participants and believe it has the potential to make the digital sphere a safer place for personal data. But it has to challenge numerous difficulties complying with the GDPR. The ideas put forward in this paper might serve as a starting point to substantiate the principle of Privacy by Design (Art. 25 GDPR) for the practical use of blockchain technology.

There is one more rather political question to consider in discussing "Privacy by Design." To fully adopt and implement the paradigm of "Privacy by Design," we must recognize transparency as an important attribute of not only the data itself but also the code handling the personal data (open-source). Knowing what a system does with our data is the only way of allowing educated data subjects to identify risks themselves. For this reason, we have deliberately chosen to represent the concept of the data subject's consent such that the responsibility of providing personal data lies, both legally and technically, in his or her own hands. By representing the consent of the data subject in a smart contract ecosystem, we make the processing of personal data a question of control rather than trust. Additionally, we are proposing the design of Test Suites, which allow for a technical verification of compliance to the GDPR of source-code.

The idea proposed in this paper goes beyond a mere reconceptualization of data handling. In times of the emerging Web3.0 and key features of decentralized ledgers, consensus-based transaction endorsement, and trust through transparency instead of accountability, we want to also introduce a new way of thinking about how our IT-systems interact with each other and how we should evaluate data locality and validity. From a technical perspective, the results of our work bear certain similarities to those in [12], indicating that the legal requirements of the GDPR indeed ask for a reconceptualization of data handling that could finally become feasible for the mainstream internet-user. We envision a near-future scenario in which self-hosting one's personal data is as routine as logging in to Facebook. In their paper, [12], Zyskind et. al. showed how a system might be designed that not only aligns with our proposed architecture but also manages to track access to personal data on behalf of the data subjects on a blockchain. From the perspective of constitutional law, we believe that blockchain technology can raise the status quo to the ideal of data self-sovereignty for every citizen in comparison to the current design of the digital world. In other words: a high degree of blockchain-based informational self-determination would allow our digital Alter Ego to become what it's supposed to be: Ours.

ACKNOWLEDGMENTS

The authors acknowledge the very helpful copy editing of Saga Briggs. Michael Kolain would like to thank Prof. Dr. Mario Martini for his support. Christian Wirth would like to thank Anja Grafenauer for her support.

REFERENCES

1. Giuseppe Ateniese, Bernardo Magri, Daniele Venturi, and Ewerton Andrade. 2017. Redactable blockchain–or–rewriting history in bitcoin and friends. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*. IEEE, 111–126.
2. Ulrich Baumgartner and Tina Gausling. 2017. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. In *Zeitschrift fÃijr Datenschutzrecht (ZD)*. IEEE, 308–313.
3. Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 15–29.
4. Reiner BÃűhme and Paulina Pesch. 2017. Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie. In *Datenschutz und Datensicherheit (DuD)*. 473–481.
5. Elke Kunde, Dr. Markus Kaulartz, Med Ridha Ben Naceur, Samater Liban, Matthias Kunz, Prof. Dr.-Ing. Volker Skwarek, Prof. Dr.-Ing. Katarina Adam, Rebekka Weiß, and Marco Liesenjohann. 2018. Faktenpapier Blockchain und Datenschutz. (2018), 40. https://www.bitkom.org/noindex/Publikationen/2018/Leitfaeden/180222-Faktenpapier-Blockchain-und-Datenschutz.pdf
6. Jonathan Katz and Yehuda Lindell. 2014. *Introduction to modern cryptography*. CRC press.
7. Bert-Jaap Koops and Ronald Leenes. 2014. Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the ‘Privacy by Design’ Provision in Data-protection Law. *Int. Rev. Law Comput. Technol.* 28, 2 (May 2014), 159–171. DOI: http://dx.doi.org/10.1080/13600869.2013.801589
8. Ora Lassila and James Hendler. 2007. Embracing" Web 3.0". *IEEE Internet Computing* 11, 3 (2007).
9. Mario Martini and Quirin Weinzierl. 2017. Die Blockchain-Technologie und das Recht auf Vergessenwerden. *Neue Zeitschrift für Verwaltungsrecht (NVwZ)* (2017), 1251 – 1259.
10. Christian Wirth and Michael Kolain. 2016. Speed Dating on Smart Contracts. In *Proceedings of the International Conference for E-Democracy and Open Government*. Parycek/Edelmann (eds.), 201–204.
11. Christian Wirth and Michael Kolain. 2017. Multichain Governance. In *Recht 4.0, Innovationen aus den rechtswissenschaftlichen Laboren*. Oldenburger Verlag fÃijr Wirtschaft, Informatik und Recht, 833–845.
12. Guy Zyskind, Oz Nathan, and others. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 180–184.