Blockchain and the GDPR's right to erasure

David van de Giessen
University of Twente
PO Box 217, 7500 AE Enschede
the Netherlands
d.r.vandegiessen@student.utwente.nl

ABSTRACT

The purpose of this paper is to discuss whether it is possible to reconcile blockchain with the requirements of article 17 of the General Data Protection Regulation (GDPR), the right to erasure. This paper includes a literature research on the different technical and governance approaches to become compliant with the GDPR. The results of this literature research are compared with experiences in the work field. This work will identify the approaches, evaluate the strengths and weaknesses of the approaches and give guidelines on how blockchain can be used compliant with the GDPR. These guidelines can help to manage data and use blockchain technology in a correct manner. The guidelines are meant for the design of new blockchain driven solutions and will thereby not address challenges for existing blockchain applications.

Keywords

Blockchain, Right to erasure, GDPR, privacy by design, data protection, technical enforceability, governance enforceability

1. INTRODUCTION

The amount of data is growing rapidly the last few years. According to ScienceDaily [19], 90% of the world's data is created in the last two years. Data is constantly being collected and used for improvements, innovation and economic value. Though, the public concern about privacy is growing. The citizens, called data subjects from now on, have almost no control about what data is stored and what the data is used for. Furthermore, the data subjects do not know how the data is stored. The GDPR is introduced to give data subjects control over data about them. Data subjects have several rights, such as the right to erasure. These new rights let new challenges arise for companies that store and use data.

Blockchain is a technology to store data. It is a distributed ledger, which means that there is no central database with all the data. The data is replicated and shared among all participants. Data is stored in blocks that are immutable: new data can be added to the blockchain, but once the data has been added, it cannot be changed or removed anymore. The distribution and immutability aspects of blockchain technology lead to challenges in becoming compliant with the right to erasure of the GDPR. When there is personal data present on a blockchain, there must be a way to remove the data from the blockchain.

Several approaches emerged in becoming compliant with the GDPR. Though, all these approaches have some problems and are unfit to deal with the erasure of personal data in blockchains [16]. Tradeoffs between GDPR compliancy and blockchain value have to be made. The following research question has been derived:

How can blockchain driven applications be compliant with the GDPR's right to erasure?

In order to solve this problem, three sub research questions need to be answered:

- *What are the conceptual technical approaches to overcome the problem of blockchain with right to erasure?*
- *What are the most important governance measures needed to be compliant with the right to erasure?*
- *What technical approaches and governance measures fit best with the guidelines of organizations?*

The first part of the paper gives insight in the core concepts used in this paper. Blockchain technology, the GDPR and the right to erasure are discussed. The second part of the paper is a literature study on the technical and governance approaches. The last part of the research is the validation of the results of the literature study and a consideration about what approach companies should use in their blockchain driven applications.

2. METHODOLOGY

The first part of the research will be a literature research. The fields of research will be:

- Technical approaches to meet the right to erasure
- Governance measures to meet the right to erasure

In the chosen articles, the most important concepts are listed and put into a table. The concepts that are mentioned most are chosen and worked out in the paper. The criteria for inclusion/exclusion will be as followed: For the approaches to meet the right to erasure, only papers published in 2016 or later will used. This ensures that all approaches match the GDPR and no other privacy law. For methods of making a blockchain mutable, no papers prior to 2010 will be used, which ensures that the research is up to date.

The results of this literature study will be validated by companies that have experience in blockchain technology and know the challenges it has with the GDPR. The method of this field research will be qualitative interviews. This ensures that a good understanding of company's motives and actions are achieved.

The two main questions in this interview are:

- What technical approaches are used or preferred to be compliant with the GDPR's right to erasure?
- What governance structures are used in order to be compliant with the GDPR's right to erasure?

31th Twente Student Conference on IT, July 5th, 2019, Enschede, The Netherlands.

3. BACKGROUND

In order to understand the solution approaches, a clear understanding on what blockchain technology is and how it works is needed. The core concepts of blockchain technology are explained below. Furthermore, the GDPR and its right to erasure are explained.

3.1 Blockchain

Blockchain technology is used to store data. According to Christidis and Devetsikiotis [4], Blockchain is "a distributed data structure that is shared among members of a network". All members, which are called nodes, on the blockchain have access to the data and have its complete history saved in their own database (ledger). Every party verifies the transactions of itself and of all transaction partners, without an intermediary. [10]

Blockchain is, as the name suggests, a chain of blocks. Each block carries a set of data and a hash that corresponds to the previous block. This creates a link between blocks, thus creating a chain of blocks [4]. Once a party communicates a certain transaction into the peer-to-peer network, the transaction needs to undergo a verification process. This verification is performed by miners that devote computer power to verify the transaction [15]. New transactions are only accepted by other nodes in the network if the transaction is valid and the transaction inputs are not spent yet.

Once the block is verified by the nodes and added to the chain, information in the block can no longer be changed [21]. The data in a blockchain is organized in an append-only ledger, which means that the data cannot be taken out [14].

There are different types of blockchains. Originally, blockchain was used for Bitcoin [14]. This is an example of a public blockchain. Everyone is allowed to become a participating node. Opposite to this public, 'permissionless', type of blockchain network is the permissioned blockchain, where access to the network needs to be granted before a node is able to join the network.

The main features of blockchain can be summarized as follows [12]:

- *Decentralization:* Trust is spread across multiple participants. The integrity of data is governed by many so-called decentralized parties.
- *Immutability:* Once sufficient participants agreed and data is added to the blockchain, the information is stored immutably.
- *Scalability:* A large amount of participants leads to a high throughput. This can be limiting for applications that need a high throughput.
- *Limited privacy:* Data is visible to and stored by all participants in a blockchain. Permissioned blockchains limit the amount of participants and thereby the rate of disclosure.

3.2 GDPR

The General Data Protection Regulation (GDPR) is the latest regulation in the European Union in order to protect the data of its citizens and went into application in 2018. Companies and all their information systems have to cope with this new privacy law. The GDPR is developed in order to improve the level of personal data protection in present-day digital environment [20]. In comparison with the previous data protection law (DIR95), the scope of the GDPR has extended. This extra-territorial reach [13] means that the GDPR does not only apply to companies that control and process data in the European Union, but it also applies to controllers and processors that are not established in Europe if they offer goods or services to European citizens or if they monitor the behavior of individuals in Europe. [13]

Lyons at al [14] describe personal data as the heart of the GDPR. The GDPR applies to all personal data of European citizens. Data that does not directly identify a person but identifies a person by the use of additional available information can be considered as pseudonymous data (Recital 26 GDPR). Pseudonymizing data is a step in the right direction, but it still results in personal data, since it is not completely anonymous. Therefore, the GDPR also applies to pseudonymous data. [13]

Three main actors can be identified in the GDPR [14]:

- **Data subject**. The data relates to this person.
- **Data controller**. The natural person or public authority that determines the purposes and means of the processing of personal data. The data controller is ultimately accountable for GDPR compliancy.
- **Data processor**. The data processor 'processes data on behalf of the data controller'.

One of the newly introduced terms in the GDPR is accountability [20]. Data controllers and data processors are held accountable for GDPR compliancy. Furthermore, the GDPR will require companies not just to comply, but also to be able to show compliancy. [13] The GDPR states that personal data should be processed 'lawfully, fairly and transparent' (Art. 1 GDPR). This means that the data controller has to have legal grounds to collect the data and has to be transparent about how it intends to use the data [14]. Protecting privacy should be a default setting of the underlying information systems. This is called privacy by design (Art. 25 GDPR). The controller has to ensure that only necessary data is gathered and processed.

One of the key aims of the GDPR is to empower individuals and give them control over their personal data [13]. Data subjects have to give consent to let their personal data be collected and have several rights, such as the right to access, the right to erasure and the right to data portability. Individuals can exercise this rights for free. As a company, you must respond within a month.

Since many data breaches have occurred in the past, the GDPR requires the controller to notify a data breach to a supervising authority [6]. Companies need to improve their cybersecurity efforts to protect data of individuals in order to minimize liability under the GDPR. The GDPR also obliges controllers to notify data breaches to the corresponding data subjects.

The most important principles of the GDPR can be summarized as follows:

- The GDPR applies to all data that can be used to (indirectly) identify individuals.
- Data controllers and processors are accountable for GDPR compliancy.
- Data subjects are empowered by several rights in order to control their own privacy.

3.3 Right to erasure

Article 17 of the GDPR mandates that data subjects shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. Data controllers are obliged to delete this data when one of the following conditions applies:

(a) Personal data is no longer necessary for the purposes it was collected or processed

(b) The data subject withdraws the consent on which the processing is based

(c) The data subject objects the processing and there are no overriding legitimate grounds for processing

(d) The data has been unlawfully processed

(e) Personal data has to be erased for compliance with a legal obligation

(f) The personal data has been collected in relation to the offer of information society services to a child under 16 years of age

The right to erasure is also known as the 'right to be forgotten'.

4. BLOCKCHAIN AND THE RIGHT TO ERASURE

Becoming compliant with the GDPR requires technical solutions. The blockchain applications need to be designed and implemented in a way it provides privacy as a default. This is called *technical enforceability*. Though, not only technical solutions are needed. Organizations need to manage their information in a structured and safe way. The way this information is managed is called *information governance enforceability*. Different approaches in the technical and governance enforceability can be recognized.

4.1 Technical enforceability

This literature review on the technical approaches follows the guidelines of Webster and Watson [22]. The results of this literature research can be found in table 1.

The articles and journals used in this literature research are found using forward and backward tracking in articles found using combinations of *Blockchain, GDPR, privacy* and *Right to erasure* as search terms. The most relevant (eight) sources of literature are chosen. The recognized concepts are elaborated below.

4.1.1 General

The GDPR applies to personal data. It states that personal data shall only be collected for specified, explicit and legitimate reasons. (Art 5 GDPR) No more data than needed can be stored in databases. The tension between blockchain driven applications and the GDPR only occurs when these applications are saving personal data. If storing personal data is not needed, these challenges are not needed to overcome. For the rest of this research, we focus on blockchain driven applications that try to store personal data of individuals.

4.1.1.1 Encrypting and hashing

Encrypting and hashing are both fundamental to blockchain technology. Hashing data means transforming it into an unreadable piece of data. Hashing a certain value always results in the same hash string. Restoring to the original value is not possible. Encrypting the data is making the data unreadable using an encryption key. The data can be decrypted and read using the same encryption key. [9] Lyons et al [14] describe hashed personal data as a grey area. If the advanced hashing algorithms are used in combination with 'salting' or 'peppering' these hashes, which involve adding extra information to the data, it is very unlikely that a brute force attack can reverse the data.

In article 17 of the GDPR, the term 'erasure of data' is mentioned several times. There is no explanation in the GDPR of what the term erasure of data actually means. [9] If encrypted data without storing the encryption key can be considered as erasure, personal data can be stored on a blockchain (in the current implementation of the blockchain), even though it is not deletion of data in the strictest sense.

4.1.1.2 Storage principles

In centralized databases, the basic database operations are often described as CRUD. [9] CRUD stands for *create, read, update* and *delete*. In a blockchain, blocks of information can not be updated or deleted. Therefore, CRUD does not match with decentralized ledger technologies. Instead, blockchain operations can be described as CRAB. CRAB stands for *create*,

Table 1. Literature research technical approaches

	General	*Access*	*Anonymization*		*Blockchain as access control*	*Mutability*	
Publication	What is erasure	Revoke access rights	Key destruction	Quantum resistant encryption	Off-chain	μchain	Chameleon
[9] Van Humbeeck, A.	x		x		x		
[16] Pagallo, U.	x		x		x	x	x
[14] Lyons, T.	x		x	x	x		x
[3] Chang, H.			x		x		x
[1] Ateniese, G.							x
[5] Finck, M.	x		x				x
[7] Hofman, D.		x					
[11] Ibáñez, L.			x		x		x

read, *append* and *burn*. Append replaces the update operation. By appending a new block to the blockchain, the 'world state' is changed. [9]. The world state is the sum of all operations until now. The burn operation replaces the delete operation. The burn operation consists of stopping the ability to transfer the asset by throwing away the encryption key. The data itself is never deleted. CRAB cannot help with being compliant with the GDPR. The data is not deleted and it can not be proven that the encryption keys are lost by the data controllers.

4.1.2 Approaches

In table 1, three main approach categories can be recognized: *anonymization*, *blockchain as access control* and *mutability*. These approaches are elaborated below.

4.1.2.1 Anonymization

One approach in removing personal data from the blockchain is making it unreadable. This approach is called "key destruction". Personal data is encrypted. Whenever a data subject uses its right to erasure of personal data, the encryption key is thrown away. [16] This results in encrypted data on a blockchain that can not be decrypted anymore.

As mentioned in section 4.1.1.2, there is no clear definition in the GDPR on what erasure of data means. Taking the growing power of brute force attacks and advances in technology into account, interpreting erasure of data the conservative way seems to be the safest way. For this approach, the clash appears more as a matter of security. A pro of this approach is that main structure of blockchain applications can remain the same, which results in remaining the core values of blockchain technology. The data is still distributed and the blocks are still immutable.

4.1.2.2 Blockchain as access control

According to Van Humbeeck [9], saving data *off-chain* is a popular option to get around the challenges of blockchain and the GDPR. Personal data is stored under the control of identifiable data controllers and not on the blockchain. [16] The blockchain acts as an access control point. On the blockchain, a link to the data is stored together with the hash of the data. To see how this works on a permissioned blockchain, consider the following situation based on the off-chain example of Van Humbeeck [9], which is shown in figure 1. Suppose company 1 wants to retrieve information about company 2.

1. Company 1 wants to retrieve information about company 2. It does not know where the information about company 2 is stored. It sends a request to the blockchain for the specific data.
2. The blockchain verifies if the requestor (company 1) has proper authorization. If company has proper authorization, it gets the link to the personal data and the hash of the corresponding data.
3. Company 1 uses the link to get direct access to the backend of company 2. It retrieves the information.
4. Company 1 checks if the information is correct by hashing it and comparing it to the hash saved in the blockchain. If the hashes match, the information is correct.

Whenever the data subjects want their personal data to be erased, the data can be removed from the local databases. The link and hash in the blockchain become useless. As described in section 4.2.1.1, hashed personal data is a grey area regarding to the GDPR.

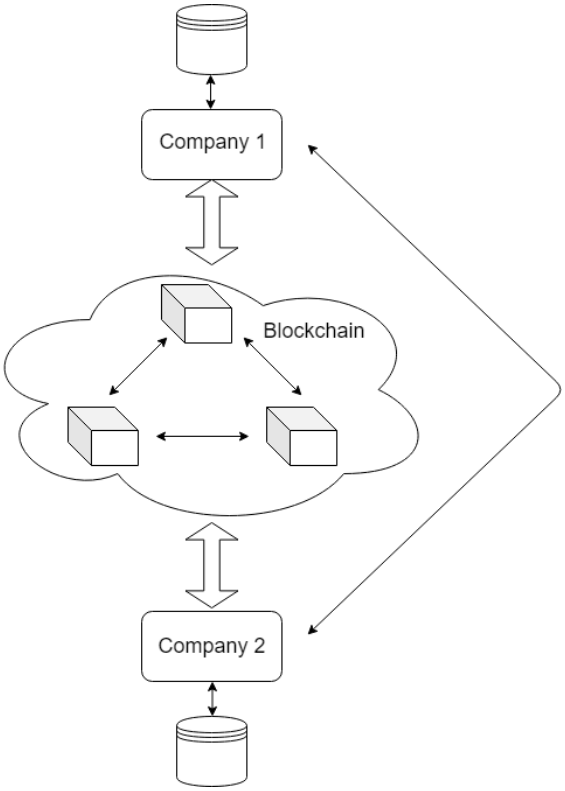

Figure 1. Off-chain structure

The biggest pro of this approach is that it is completely GDPR compliant. The right of erasure can be called without any problems. Though, the price of this solution is high. The decentralization principle is betrayed. Van Humbeeck [9] describes the cons:

- Less transparency. No one knows exactly who accessed the data. Access tokens can be added to the link to maintain control about the amount of times the retrieved link is used. This increases the complexity of the implementation.
- The benefit of data-ownership is reduced. Once the data is stored off-chain, it is not clear who is the controller of the data.
- Point-to-point integrations between companies' backends are needed. For every new partner, a new integration with all the existing members should be added.
- More attack vectors. All data controllers have their own database, application and technological landscape. The risk of a potential breach of part of the personal data increases.
- Reduced queryability. It becomes impossible to search to data that is spread across multiple off-chain databases.
- Added complexity. The risk of errors and bugs increases.

Furthermore, this approach is unfit to deal with existing blockchains. It only works for setting up new blockchain environments.

4.1.2.3 Mutability

The third approach concerns the mutability of a blockchain. Whenever a blockchain becomes mutable, data can be updated and removed from a blockchain.

Some projects are exploring the use of chameleon hashes. The aim of this approach is to make redactable blockchains.[16] Hash functions that involve a trapdoor are used. This trapdoor allows rewriting a block of information under specific constraints. The redaction can be performed by trusted third parties or by adding a hash function as a primitive of the blockchains protocol. [16] A marker will be put on the block to say that the block is edited. [3] Another, less mentioned, way of making the blockchain mutable is called μchain [17].

Whenever a block becomes editable, personal data can be erased from the block. Thereby, this solution becomes GDPR compliant. Though, the price for this solution is high. The value of immutability and thereby trust is reduced by letting parties edit the blocks. Furthermore, Pagallo et al [16] mention that critics call it "betrayal of the decentralization principle". This is also not a solution for existing blockchains, since blockchains need to include the chameleon hash functions from the beginning of their existence in order to be redactable.

4.2 Information governance enforceability

Becoming compliant with the GDPR does not only require development of technical solutions. It requires information governance. Smallwood defines information governance as an all-encompassing term for how an organization manages the totality of its information. [18] It is a set of policies, processes and controls to manage information in compliance with external regulatory requirements and internal governance frameworks. In this case, the GDPR is the external regulatory. It requires data controllers and processors to be able to erase data of data subjects.

Beckett (2017) states that the most important thing to comply with the GDPR is that you simply know where and how all the data is stored. [2] Whenever someone makes a request to erase all his personal data, you need to have a clear overview of all the places where the data could be stored. In order to do this, a clear overview of the database structures needs to be present. Furthermore, Beckett states that you do not only have to know where and how the data is stored, but also all the ways it is processed. The different ways in which data and documents are handled must be recorded strictly.

Data controllers and data processors need to have their responsibilities and procedures clear. Whenever a data subject uses his right to be forgotten, it has to be clear who is responsible for the deletion of the data. The steps that this responsible person needs to take have to be clear in order to erase the data accurately and in-time.

Ensuring that a blockchain application meets regulatory needs requires thoughtful design up front. [7] This means that privacy is something that should be taken into account from the start in all layers of the system and their interactions. Developers should have privacy as a focus point instead of seeing it as a constraint.

Transparency is one of the keywords in the GDPR. Article 5 of the GDPR states that data shall be processed in a transparent manner in relation to the data subject. As a controller or processor, you have to be able to proof how the data is used and how you are going to erase data if needed. This also requires accuracy: the data should be erased in-time. [8]

5. VALIDATION AND SOLUTION GUIDELINES

5.1 Validation

The results of the literature research are validated by interviewing experts in the field of blockchain applications. These experts have experience in the development of blockchain applications and are facing the challenges of the GDPR. The results of this validation are discussed below.

5.1.1 Technical approaches

The first insight in this research is that a clear evaluation of the role of blockchain technology is needed. The goal of the use of blockchain technology is that it helps people in doing their job. The blockchain takes over communication and verification. When creating a blockchain driven application, you should look to the goal of the use of blockchain rather than following the blockchain philosophy perfectly. An example of this is the role of trusted third parties. Following the philosophy of blockchain, trusted third parties are 'not needed' anymore. Though, if you want to have a representation of the world in a blockchain, a trusted third party is needed.

GDPR compliancy is seen as a continuous scale and not a discrete scale. Organizations will have a hard time in becoming completely compliant with the right to erasure. Therefore, the main goal of these organizations is to become as compliant as possible and reasonable. This includes having privacy as a focus point in your organization and having technical and organizational measures in order to be as compliant as possible. The three main technical measures discussed in the literature are evaluated by the experts and discussed below.

- Key destruction is seen as not enough for right to erasure. The growing brute force decryption powers make this way of erasure a risk for the future. The conservative way is preferred and this solution is seen as insufficient. The experts agree on that you should never save personal data on a blockchain.
- Off-chain storage is seen as the most elegant option to become compliant with the right to erasure. In this solution, personal data is not saved on a blockchain. On the blockchain, an unrelatable hashed private key is saved. This unrelatable key can be translated off-chain by a database or just by 'knowledge in the company'. This off-chain storage approached is seen as the most elegant option because it ensures that there is no personal data on the blockchain and thereby the GDPR compliancy can be achieved. The blockchain can still be used in its power: automated verification and decision making. The information on the blockchain can still be trusted.
- Mutating a blockchain is seen as technically interesting, but it is difficult to prove that the data is actually removed from the blockchain. Furthermore, one of the core principles of blockchain is that nodes have agreed on information on the blockchain and can be held accountable for this agreement. Making a blockchain mutable undermines this accountability argument. Mutating the blockchain is seen as a last resort for organizations to become compliant and is thereby seen as less elegant than off-chain storage of data.

One can conclude that storing data off-chain is the most preferred approach. This helps in anonymizing data on a blockchain. Though, only direct personal data is anonymized. Direct personal data is data that can directly identify persons, such as names, addresses, etcetera. It is still possible that a person can be identified by indirect, pseudonymous, personal data, such as patterns. People's lifestyle can be identified if you follow the traces of information. For example, a certain key can interact at specific moments on specific places with specific people. You do not know who this is, but the pattern of lifestyle can help to identify this person. This can also be seen as personal data. Whenever the direct personal data is stored off-chain, indirect personal data can still be present on the blockchain. This traces of personal data can be interrupted by the use of wallets. A wallet is a set of keys a certain participant uses. The participant uses different keys for different transactions. Which key belongs to which person is saved off-chain. This makes it harder, if not impossible, to identify the person.

5.1.2 Information governance

In the interviews, 5 main steps in facing the challenge of the right to erasure emerged. These steps are the following:

- Create a clear process for data subjects on how they can use their right to be forgotten. This can be a platform or process using emails. It must be clear for the data subjects how they could use the right and what the procedures are.
- Know where and how the data is stored and processed. Whenever the right is used, it must be clear where the data is stored. You have to know where the data is stored and used in order to erase it.
- Clear responsibilities within the organizations. Whenever the right is used, it has to be clear who is responsible for what actions of erasure.
- Clear procedures for the erasure. The responsible person needs to know what to do when the right is used. Where can you find the data? How do you erase it?
- Clear agreements with participating parties. The parties that participate in the blockchain network need to agree on the erasure procedures in the network.

One big challenge of the GDPR is that you do not only have to erase the data, but also have to show and prove that the data is erased. It will always be hard for companies to show that data is not present anymore. Though, clear procedures and technical approaches help in climbing up the transparency spectrum of GDPR compliancy.

5.2 Solution guidelines

The goal of this paper was to identify ways to become compliant with the GDPR's right to erasure. In the literature research and validation, several technical and organizational guidelines emerged. These together form the solution guidelines.

The following guidelines for the technical enforceability can be used.

- Never save personal data directly on a blockchain
- Save unrelatable hashed data on a blockchain and save relatable (personal) data off-chain
- Encrypt all data that you control or process
- Use methods to make data more unreadable such as private key wallets

The following guidelines for the governance enforceability can be used

- Have a transparent and clear procedure for data subjects on how they could use the right
- Know where and how data is stored and processed
- Have clear responsibilities for the erasure process
- Have a clear process for the erasure of data
- Have transparent agreements on the process of erasure with all participating parties.

6. CONCLUSION

GDPR compliancy is not a discrete spectrum, but a continuum. Organizations have to do their best in order to become as most compliant as possible and have to take technical and organizational measures.

The first research question discussed the technical approaches in becoming compliant to the GDPR's right to erasure. The main technical approaches are throwing away encryption keys, saving personal data off-chain and making the blockchain mutable. None of the approaches is completely fit for this challenge if the requirements of being completely GDPR compliant and keeping all the core values and principles of blockchain philosophy are held.

The second research question discussed the governance approaches in becoming compliant to the GDPR's right to erasure. The answer to this question is that organizations need to have a clear overview of all the data they control and process and that they have to have clear procedures and responsibilities within the organization and with the complete network. Furthermore, transparency in these processes is important.

The third question is a validation of the two previous questions. The off-chain storage of data is seen as the most elegant option to become as compliant as possible with the GDPR guidelines. You should never save data on a blockchain. This technical solution goes hand in hand with the governance solutions mentioned above. This is also the answer to the main research question: taking technical measures and organizational steps is key to become compliant with the GDPR's right to erasure.

7. DISCUSSION AND FUTURE WORK

In the literature research and field validation, the research focusses on finding a way to implement new blockchain solutions compliant with the GDPR's right to erasure. These solutions are not fit for existing blockchain applications. In the future, research can be done on whether existing blockchain applications can be compliant with the GDPR and if the answer is yes, how they can be compliant.

The research mainly focusses on direct personal data and not on data created by patterns in the blockchain. The use of wallets, mentioned in section 5.1 and 5.2, is a potential solution to overcome the problem of personal data by traces. There is almost no literature research conducted on how to overcome this problem. Therefore, it is an interesting question in future research to do research on what to do with traces as personal data in blockchains.

The field research resulted in various insights into the problem. The main consensus is that a discrete compliant version of blockchain has not been found yet. The reasons for this consensus can be the low number of interviewed experts or the fact that the GDPR went into force only a year ago. Organizations are still working on their GDPR compliancy.

8. ACKNOWLEDGEMENTS

The author thanks Simon Dalmonen for the valuable feedback, insights and coaching during the process of doing this research. Furthermore, the author thanks all the participants from the interviews.

9. REFERENCES

[1] Ateniese G. et al. 2017. Redactable blockchain–or–rewriting history in bitcoin and friends. *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on. IEEE, 111–126*. Retrieved from https://eprint.iacr.org/2016/757.pdf

[2] Becket, P. et al. 2017. GDPR compliance: your tech's department's next opportunity. *Computer, Fraud and Security, 5, 9-13.* DOI = https://doi.org/10.1016/S1361-3723(17)30041-6

[3] Chang, H. 2017. Blockchain: Disrupting Data Protection? *University of Hong Kong Faculty of Law Research Paper No. 2017/041.* Available at SSRN: https://ssrn.com/abstract=3093166

[4] Christidis, K. and Devetsikiotis, M. 2016. Blockchains and Smart Contracts for the Internet of Things. *In IEEE Access, Vol. 4. 2292-2303.* DOI = https://doi.org/10.1109/ACCESS.2016.2566339

[5] Finck, M. 2017. Blockchain and Data Protection in the European Union. *Max Planck Institute for Innovation & Competition Research Paper No. 18-01.* DOI = https://doi.org/10.2139/ssrn.3080322

[6] He, L. et al. 2019 The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management, 22:1, 1-6*, DOI = https://doi.org/10.1080/1097198X.2019.1569186

[7] Hofman, D. et al. 2019. "The margin between the edge of the world and infinite possibility". *Records Management Journal, 29(1/2), 240-257.* DOI = https://doi.org/10.1108/RMJ-12-2018-0045

[8] Hristov, P., Dimitrov, W. 2018. The blockchain as a backbone of GDPR compliant frameworks. Retrieved from https://www.researchgate.net/publication/328576742

[9] van Humbeeck, A. 2017. The Blockchain-GDPR Paradox. *Journal of Data Protection & Privacy, 2(3), 208-212*

[10] Iansiti, M. and Lakhani K. R. 2017. The truth about blockchain. Retrieved from URL https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf

[11] Ibáñez, L. et al. 2018. On Blockchains and the General Data Protection Regulation. *University of Southampton.* Retrieved from https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf

[12] Knirsch, F. et al. 2019. Implementing a blockchain from scratch: why, how and what we learned. DOI = https://doi.org/10.1186/s13635-019-0085-3

[13] Linklaters. The General Data Protection Regulation: a survival guide. 2016. Available from: https://www.linklaters.com/nl-nl/insights/publications/2016/june/guide-to-the-general-data-protection-regulation. Accessed 17 May 2019.

[14] Lyons, T. et al. 2018. Blockchain and the GDPR. Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

[15] Nofer, M. et al. 2017. Blockchain. DOI = https://doi.org/10.1007/s12599-017-0467-3

[16] Pagallo U.2018. Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure. DOI = https://doi.org/10.3233/978-1-61499-935-5-81

[17] Puddu, I. et al. 2017. μchain: How to Forget without Hard Forks. Retrieved from https://eprint.iacr.org/2017/106.pdf

[18] Smallwood, R.F. 2015. Information Governance: Concepts, Strategies and Best Practices, DOI = https://doi.org/10.1002/9781118433829

[19] ScienceDaily. Big data, for better or worse: 90% of world's data generated over last two years. 2013.

[20] Tikkinen-Piri, C. et al. 2018. EU general data protection regulation: changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153

[21] Wirth, C. and Kolain, M. 2018. Privacy by Blockchain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data

[22] Webster, J., Watson, R.T., 2002. Analyzing the Past to Prepare for the Future: *Writinga Literature Review 26, 13-23*