University of Bern

How can Privacy considerations be consolidated with transaction transparency?

Computer Science and Private Law

Supervisors: Prof. Dr. Christian Cachin, Prof Dr. Mirjam Eggen, Dr. Christian Sillaber

Date of Submission: 22. April 2022

Authors: Marius Asadauskas, Lynn Grau

Addresses: Murtenstrasse 143e, 3008 Bern

Sulgenheimweg 17, 3007 Bern

Matriculation number: 18-106-575, 18-109-629

E-Mail: [marius.asadauskas@students.unibe.ch](mailto:marius.asadauskas@students.unibe.ch)

[lynn.grau@students.unibe.ch](mailto:lynn.grau@students.unibe.ch)

Index

[Legal Bibliography III](#_Toc101513029)

[Technical Bibliography V](#_Toc101513030)

[List of abbreviations VII](#_Toc101513031)

[1 Introduction 1](#_Toc101513032)

[2 Privacy and Blockchain Types 2](#_Toc101513033)

[2.1 Personal, anonymous and pseudonymized data 2](#_Toc101513034)

[2.2 UTXO vs Account Based Blockchains 2](#_Toc101513035)

[3 Privacy in Different Cryptocurrencies 3](#_Toc101513036)

[3.1 Bitcoin 4](#_Toc101513037)

[3.1.1 Address Reuse 5](#_Toc101513038)

[3.1.2 Bitcoin Mixers 5](#_Toc101513039)

[3.1.3 Violating your own privacy in Bitcoin 5](#_Toc101513040)

[3.2 Privacy Coins 6](#_Toc101513041)

[3.3 Monero 6](#_Toc101513042)

[3.3.1 Violating your own privacy in Monero 7](#_Toc101513043)

[3.4 Z-Cash 8](#_Toc101513044)

[3.4.1 Violating your own Privacy in Z-cash 9](#_Toc101513045)

[4 Data Privacy Regulations and public permissionless Blockchains 10](#_Toc101513046)

[5 Tensions between the GDPR and public permissionless Blockchains 11](#_Toc101513047)

[5.1 Legal grounds for data processing 13](#_Toc101513048)

[5.2 Stakeholders 14](#_Toc101513049)

[5.3 Legal grounds 17](#_Toc101513050)

[6 Implementation of Data Subject Rights in Blockchains 19](#_Toc101513051)

[7 Anticipated Problems with public permissionless Blockchains regarding the revADP 21](#_Toc101513052)

[8 Conclusion 22](#_Toc101513053)

[Declaration of Authorship 23](#_Toc101513054)

Legal Bibliography

Baeriswyl Bruno: Der «grosse Bruder» DSGVO und das revDSG: Ein vergleichender Überblick, SZW 2021, S. 8 -15.

Daniel Erik/Elias Rohrer/Florian Tschorsch: Map-Z: Exposing the Zcash Network in Times of Transitions, arXiv:1907.09755v2 [cs.CR] 26 Jul 2019 available under: <https://www.researchgate.net/publication/334644591 \_Map-Z\_Exposing \_the\_Zcash\_Network\_in\_Times\_of\_Transition>.

Kappos George/Yousaf Haaroon/Maller Mary/Meiklejohn Sarah: An Empirical Analysis of Anonymity in Zcash, ISBN 978-1-939133-04-5 August 2018, available under: <https://www.usenix.org/system /files/conference/usenixsecurity18/sec18-kappos.pdf>.

Eichler Natalie /Jongerius Silvan/McMullen Greg/Naegele Oliver/ Steininger Liz / Wagner Kai: Blockchain, data protection and the GDPR: < https://www.crowdfundinsider.com/wpcontent/uploads/2018/06/GDPR\_Position\_Paper\_v1.0.pdf>.

European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), Study, STOA, Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law?, PE 634.445, July 2019, available under: <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS\_STU(2019)634445\_EN.pdf>.

Keller Claudia, Datenschutz, 1. Grundlagen des Schweizer Datenschutzrechts, 4. Outsourcing von Datenbearbeitungen an Dritte, Zürich 2019, p. 9-25, available under: <https:// www.swisslex.ch/doc/bookdoc/3c5007f0-c6be-489492a130d3a353d37e/>.

Plattner Matthias, Datenschutzrechtliche Herausforderungen der Distributed-Ledger-Technologie, Rechtliche Fragestellungen, Zürich 2021, p. 35-59, available under: <https://www.swisslex.ch/de/doc /bookdoc/a96ab058-ab8f-49a3-a96f-b2b0d47a3266>.

Schmid Daniel: Part B. EU Regulation § 6. Data Protection in: The Law of Crypto Assets: a handbook in Maume Phillip/Maute Lena/Fromberger Mathias (Hrsg.), München, Germany: Beck 2022. Print.

Schmid Roman/Ziolkowski Rafael/ Schwabe Gerhard: Together or Not? Exploring Stakeholder in Public and Permissionless Blockchains, Zurich Open Repository and Archive, 2022, available under: <https://www.zora.uzh.ch/id/eprint/211821/1/0595-2.pdf>.

Sorge Christoph, Anonyme Bezahlverfahren im Überblick, in: digma 2018, p. 14-17, available under:<https://www.swisslex.ch/de/doc/essay/ 60e0419d-3a44-4a60-8b27-6560 ee7c4ef6>.

Tatar Unal/Gokce Yasir/ Nussbaum Brian: Law versus technology: Blockchain, GDPR, and tough tradeoffs, computer law & security review 38 105454, 2020, available under: <https://www. sciencedirect.com/science/article/abs/pii/S0267364920300595>.

Technical Bibliography

[1] Intersoft Consulting, „Art. 4 Definitions,“ [Online]. Available: https://gdpr-info.eu/art-4-gdpr/. [Accessed on 22 April 2022].

[2] S. Nakamoto, „Bitcoin whitepaper,“ *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019),* p. 6, 2008.

[3] R. L. a. S. A. a. A. L. M. Rivest, „A method for obtaining digital signatures and public key cryptosystems,“ in *Secure communications and asymmetric cryptosystems*, Routledge, 1982, pp. 217-239.

[4] S. D. Lerner, „The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius,“ 17 April 2013. [Online]. Available: https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/.

[5] Intersoft Consulting, „Art. 17 GDPR,“ [Online]. Available: https://gdpr-info.eu/art-17-gdpr/. [Accessed on 22 April 2022].

[6] „Crypto Mixer,“ [Online]. Available: https://cryptomixer.io/. [Accessed on 22 April 2022].

[7] W. Vermaak, „https://coinmarketcap.com/alexandria/article/what-are-privacy-coins,“ 2021. [Online]. Available: https://coinmarketcap.com/alexandria/article/what-are-privacy-coins.

[8] A. Barontini, „Rings Cheatsheet,“ 1 March 2021. [Online]. Available: https://www.getmonero.org/library/RingsCheatsheet20210301.pdf. [Accessed on 22 April 2022].

[9] Monero, „Ring Size,“ [Online]. Available: https://www.getmonero.org/resources/moneropedia/ring-size.html. [Accessed on 22 April 2022].

[10] Monero, „xmrchain,“ [Online]. Available: https://xmrchain.net/. [Accessed on 22 April 2022].

[11] Bitcoinfees, „Predicting Bitcoin fees for transactions,“ 22 April 2022. [Online]. Available: https://bitcoinfees.earn.com/.

|  |
| --- |
| [12] N. a. C. R. a. C. A. a. T. E. Bitansky, „From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again,“ in *Association for Computing Machinery*, New York, NY, USA, 2012.  [13] Blockchair, “Confirmed z-z transaction,” [Online]. Available: https://blockchair.com/zcash/transaction/35f6674a1691f21aff6a3819467dbba82aaebf061d50c6ac55f39fbeae73b9a6. [Accessed on 22 April 2022]. |
| [14] Zcash, “What are zk-SNARKs?,” [Online]. Available: https://z.cash/technology/zksnarks/. [Accessed on 22 April 2022].  [15] Coindesk, “Zcash,” [Online]. Available: https://www.coindesk.com/learn/crypto/zcash/. [Accessed on 22 April 2022]. |

List of abbreviations

AML Anti Money Laundering

DLT Distributed Ledger Technology

KYC Know Your Customer

GDPR *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

revADP Federal Act on Data Protection (revised Act, 25 September 2020)

UTXO Unspent transaction output

zk-SNARKSs Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

1. Introduction

*Written by Lynn Grau*

The first blockchain was the cryptocurrency Bitcoin, has been launched in 2008.[[1]](#footnote-1) Since then, blockchain based technologies have gained a lot of popularity. The growth of DLT over the last decade has led to the recognition of the underlying technology potential of blockchain and has since been implemented in various industries such as fintech, retail, and health care. Since DLT is mainly a new way to store data, the question arises if said data is protected accordingly. In a first step the technical aspects of privacy on different blockchains will be examined. Are blockchain as anonym as they are sometimes portrayed? In the second part the legal impact of European data protection regulations on public permissionless blockchains will be examined, assessed with a case-by-case analysis from Zcash.

**Declaration of Authorship**

This work is a joint effort of the two authors Marius Asadauskas and Lynn Grau. If not specifically stated otherwise, texts were written in co-authorship (specific authorship always counts for the whole chapter). Because this paper is of an inter-faculty nature with different citations styles, to meet individual requirements we used different citations.

1. Privacy and Blockchain Types

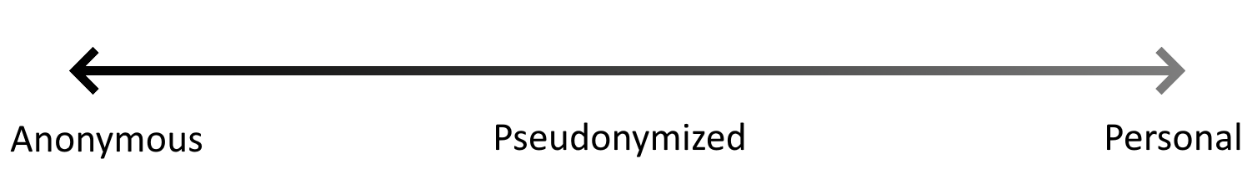
*Written by Marius Asadauskas*

* 1. Personal, anonymous and pseudonymized data

There are many types of data in our current world. Among these, the Information which concerns us as individuals the most is personal data. Personal data is defined by being linkable to a natural person through direct means. An example of this would be an individual’s unedited medical records.

Following personal data there is pseudonymized data. This refers to information, that can be linked through indirect means to a natural person. An example for this type of data would be Bitcoin’s creator, Satoshi Nakamoto, using a pseudonym while developing the cryptocurrency. If we were to link the pseudonym to an identity, we would discover plenty of personal data about said individual. Data which cannot be linked to a person through any means is anonymous data and outside of most laws. [2]

The scale of data anonymity is continuous, and data can land anywhere in between these three categories. In the case of cryptocurrencies, we are dealing with something in between anonymous and pseudonymized data.



* 1. UTXO vs Account Based Blockchains

Bitcoin was the first cryptocurrency to employ UTXO based transactions. A real-world example of UTXOs would be the use of bank checks. On a bank check you can have any amount of money but if you want to use the money, you can either use all of it at once or none of it at all. The only way to incrementally use a check would be to use all of it and then obtain a new check in return with a smaller amount. UTXO based transactions work similarly. Each UTXO contains a specific coin amount and for a transaction you can use multiple UTXO’s as input and output a UTXO for each receiver. The difference in value between the input and output becomes the transaction fee which the miner receives for their work.

On the other hand, you have account-based transactions which are most famously employed in Ethereum. Here each account is made up of an account address and a balance. In order to transfer money, you need a destination address and an amount that you want to transfer. During the transaction, your balance decreases and the destination account balance increases. This simplifies transactions and makes it easier to use wallets which collect all your assets in one place, it simplifies the implementation of smart contracts, and it allows the saving of storage space since you often reuse addresses and do not need a virtual bank check for every transaction. However, account-based cryptocurrencies create a single point of failure. If you leak a public key in UTXO based cryptocurrencies, you admit to a single or a few transactions. If you leak a public key in an account-based cryptocurrency, you leak your entire transaction history.

1. Privacy in Different Cryptocurrencies

*Written by Marius Asadauskas*

While banks and other trusted financial institutions protect their user’s privacy by releasing as little information as possible, distributed public ledgers do not have such luxury. The ledger must be accessible to everyone, and no data can be hidden. What instead can be hidden is the information held by said data. The best-case scenario happens when all the available data on a blockchain is fully anonymous. This would allow blockchains to be outside of most privacy laws. However, as we will see in the following sections, blockchains are typically pseudonymous.

The anonymization process of blockchains is done through cryptographic means. Notable methods include the use of asymmetric public and private keys, zero knowledge proofs, optimistic proofs, cryptographic hashes, and many more.

* 1. Bitcoin

Bitcoin was the first cryptocurrency developed by Satoshi Nakamoto in 2008. Already back then privacy was a big concern and hence privacy considerations were regarded while creating Bitcoin [1]. Instead of using personal data such as one’s name, address, and birthday to make a transaction, bitcoin uses public and private key pairs made within RSA encryption [3] to receive and create UTXO’s. The public key acts as an address of the UTXO and the private key acts as a password to use the UTXO.

Considering this we find the first example as to how Bitcoin is not anonymous. If we were to link a natural person to a single or multiple public keys, we would find out the transactions made by said individual. Knowing their transactions, we can find out how often they send assets, how much they own, and to which addresses they send cryptocurrency. Just by linking an individual to public keys the data on the Bitcoin blockchain becomes personal, hence bitcoin is pseudonymous.

A real-world example of how bitcoin is not anonymous would be the fact that 1.1 million Bitcoins have been linked to Satoshi Nakamoto [4]. Although Satoshi Nakamoto followed all the best privacy practices, we know that the net worth of Satoshi Nakamoto is equal to around 47 billion USD as of April 2022. If his or her real identity were to leak this would become personal data which would remain on the blockchain forever.

Considering the right to be forgotten [5] this poses a difficult issue.

* + 1. Address Reuse

It is possible to only use a single public and private key pair forever. Doing so on the Bitcoin blockchain would be the same as having the privacy of account-based cryptocurrencies without their features. A single leak of one’s public key would cause all transactions of an individual to be known and a leak of a person’s private key would cause all their assets to be in jeopardy. Hence it is strongly recommended that for each transaction you should create a new public and private key pair.

* + 1. Bitcoin Mixers

In many cryptocurrencies there are also ways to further increase privacy. In the Bitcoin network you can use Bitcoin mixers [6], which act as middlemen and take many UTXOs as inputs and forward them to their destinations. Mixers increase privacy since combining multiple UTXOs into a single transaction makes it unclear who sent which UTXO to which address. The downside of mixers is that you require a magnitude of UTXOs so that the transaction amounts do not give away the destination, see figure below. Another downside is that mixers take fees themselves and increase transaction costs even further.

Diagram

Description automatically generated

* + 1. Violating your own privacy in Bitcoin

In the Bitcoin network it is possible to mathematically prove that a transaction belongs to you. This is possible due to how RSA key pair’s function. Public keys can be used to encrypt data which only the owner of the private key can decrypt. So, if we were to send an encrypted message to an individual and they were to decrypt it, we would know that said individual has access to the private key and we would successfully link the UTXO to that person. This however requires a willingness of the owner to publicly decrypt a message.

* 1. Privacy Coins

Privacy coins are cryptocurrencies which hide transaction details from the public [7]. Transaction details which are worth hiding include sender and receiver addresses, transaction amounts, message contents and many more. Privacy coins are generally more computationally heavy, require more storage and are more complex to implement however, in return they offer a higher degree of privacy.

* 1. Monero

Monero is a UTXO based cryptocurrency which protects a transaction owners’ privacy by hiding them in a group of other possible owners. To make this possible Monero employs a mechanism called ring signatures [8]. In the Bitcoin network to use a UTXO you must include its public key and sign off with the private key. In Monero however each transaction must include exactly 11 public keys [9], with only one of the keys belonging to the UTXO owner. Furthermore, it is computationally infeasible to find out which one of the public keys belongs to the transaction leader. The amounts sent are also hidden and the receiver is hidden as well. Just looking at a Monero transaction you gain close to no information whatsoever. So contrary to Bitcoin if someone were to leak their public keys in Monero, all that would do is give them a 1 in 11 chance of being part in any transactions where the key appears.

Furthermore, in the Monero blockchain a user is forced to use one-time keys as reusing a private key more than once causes rings to be linked and the transaction to be marked as invalid. This linkage property is what prevents double spending on the blockchain. Meaning you can mathematically use a UTXO only once in Monero, while in Bitcoin you must believe that miners have validated the transactions properly.

As mentioned before privacy coins often come with downsides. In the case of Monero, ring signatures are more computationally heavy, and transactions require more storage space since you must include 11 public keys instead of just one. As of 2022 the median Monero transaction takes up 1420 Bytes [10], while the median Bitcoin transaction takes up 224 Bytes [11]. Hence the Monero blockchain is slower than the Bitcoin blockchain and consumes more storage.

* + 1. Violating your own privacy in Monero

Similarly to Bitcoin you can violate your own privacy in Monero as well, although doing so is more complicated. One way would be to include 10 much older public keys with only your own public key being relatively new in a transaction. This would make it somewhat obvious that the new public key belongs to the transaction leader.

To definitely prove that a transaction was done by you, you could try to double spend. Double spending in Monero causes the linkage property to trigger and the transaction to be marked as invalid. The linkage id together with the public key that appears twice proves that a specific transaction was done by a specific public key.

A further problem with Monero is that once a transaction becomes linked to an individual all other uses of the public key become pointless. This means that violating your own privacy in Monero causes the privacy of others to be violated as well.

* 1. Z-Cash

Z-cash is another UTXO based privacy coin. Contrary to Monero, Z-Cash uses a cryptographic method known as zero-knowledge proofs to hide transaction details. Zero-knowledge proofs are useful in proving that you know a secret without revealing the secret itself.

A simple example of a zero-knowledge proof would be Alice proving to Bob that she knows the combination to a safe. To do so Alice could firstly show the safe being closed, then secretly enter the code, and show it being opened to Bob. This way Alice has proven that she knows the safe combination without revealing the combination itself to Bob. This is a zero-knowledge proof since Alice proves the knowledge of a secret without revealing the secret itself.

In the case of Z-cash however this proof is done with complex mathematics, and proofs known as zk-SNARKs [12]. The main improvement of zk-SNARKs is that they are non-interactive. Using an interactive proof on a blockchain would be very time and resource consuming considering that some blockchains only update every 10 minutes.

Transactions in Z-cash are split up into two address types. There are transparent t-addresses and private z-addresses. It follows that four types of transactions can happen in the z-cash network. t-t, t-z, z-t, z-z. In the case of t-t transactions the blockchain acts the same as the Bitcoin blockchain. This shows us that z-cash is also pseudonymous for some users. However, users who only employ z-z transactions hide their public keys, the transaction amount, and the destination address. Simply looking at a z-z transaction reveals even less than looking at a Monero transaction, all you see is a hash [13]. Another difference between Monero and Z-cash is that in Z-cash your privacy does not depend on how careful other users are being. Furthermore, linking a public key to a natural person reveal nothing in z-z transactions. Lastly, in Z-cash privacy is a choice since you can choose t-t transactions, while in Monero privacy is the standard.

The downsides of Z-cash are similar to the downsides of other privacy coins. z-z transactions require much more computational power and the zk-SNARK proofs themselves take up hundreds of bytes [14].

A further downside is the fact that the founders own 2.1 million coins with there being a maximum of 21 million coins to ever be made. This means that a group of people hold around 10% of all the z-cash coins [15]. This fact puts the distributed nature, the morality, and the future of the cryptocurrency into question.

* + 1. Violating your own Privacy in Z-cash

Each z-z transaction comes with a commitment, which is a hash of the address to which the UTXO was sent, the amount being sent, a number which is unique to this current UTXO and a random nonce [14]. So, to violate your privacy in z-cash you must publish the data which created the commitment. If you do so, then anyone can validate that you are the owner by hashing said data and the z-z transaction then becomes a t-t transaction.

1. Data Privacy Regulations and public permissionless Blockchains

*Written by Lynn Grau*

The General Data Protection Regulation (GDPR) is a legal framework which was put into effect in 2018 for EU Members to provide a set of standardized data protection laws across all the member countries, with the goal to maintain data privacy. Even though it was drafted and passed by the EU, if organizations target data related to people in the EU, it also imposes obligations on them. Violations and non-compliance result in harsh fines, with penalties that can reach very large amount of money. [[2]](#footnote-2) The revised ADP is as the GDPR a data protection act, that aims to protect the privacy of natural people.

Many blockchains are at odds with these legal requirements. But there is not the one blockchain, rather they are to be qualified as a decentralized booking system, whose defining attribute lays in the way of storage, encryption, and verification of data safety. Thus, blockchain illustrate a class of technology, that contains many versions, who differ in complexity and their technical and governance arrangement. Therefore, it cannot be concluded if blockchains in general are compatible with the GDPR or the revADP, but a case-by-case analysis is to be assessed.[[3]](#footnote-3) However, it is harder to design a public permissionless blockchain because they lack control over which actors have access to the relevant data and do not have control over the network to treat data in a compliant manner.[[4]](#footnote-4)

Hereinafter the compatibility between the data protection acts and public permissionless blockchains will be examined, considering that a case-by-case analysis is needed and the focus in this paper is laid on privacy, the privacy-protecting digital currency Zcash (reference in 3.4) will be used as an example.

1. Tensions between the GDPR and public permissionless Blockchains

*Written by Lynn Grau*

The connecting points for the application of the GDPR are personal data and data processing. Often cryptocurrencies are seen as an anonymous payment method, this assumption has been proven above (3.1) to not hold true most of the times. To understand the concept of privacy in finance, the term anonymity needs to be defined. A technical definition of anonymity does not exist, but according to Article 26 of the GDPR data is classified as anonymous if a person cannot be identified with it. Anonymity does not just mean to exclude names but also every connection with saved data that can be used to identify a person.[[5]](#footnote-5) Data is pseudonym when appropriate technical utilities can be used, these can be decrypted and be retraced to the respective network participants. According to the prevalent, relative approach for determining the identification, only technical utilities can be used, which are for a person in charge or third party reasonably probable.[[6]](#footnote-6)

Data which is processed on the blockchains are typically: public keys, transactional data, extended content data and data saved “off-chain”. In general, public keys (similar to an account number) can with technical utilities be used to retrace the natural person, because of this they apply as pseudonym and are personal data.[[7]](#footnote-7) Other categories of data that aren’t public keys but may be used on blockchains are transactional data, such as names or addresses, contained in the payload of a given transaction. To determine if transactional data qualifies as personal data under the GDPR a case-by-case analysis needs to be assessed.[[8]](#footnote-8)

In a study of the European Parliament several solutions have been presented which have the potential to anonymize transactional data or public keys. One of these technics being zero-knowledge proofs. Zcash uses as mentioned above zero-knowledge proofs, a cryptographic method used to verify a secret.[[9]](#footnote-9) A person can prove a binary True/False statement, without having to provide access to the underlying data,[[10]](#footnote-10) if both parties use z-addresses.[[11]](#footnote-11) Z-transactions of Zcash ensure therefore that details remain hidden, even though transaction data is published on a public permissionless blockchain. Making such a transaction, neither the value, which was transferred, nor the public key is revealed, the ledger simply discloses that a transaction has been made. Zcash therefore does not process identifiable information, because it eliminates the need to track data through the transaction process. Zcash enables with zero-knowledge proofs fully anonymized transactions on the blockchain.[[12]](#footnote-12) Sk-SNARKs have the potential to facilitate compliance with article 26 GDPR the right for ‘data protection by design’ and have been considered to be compliant with the data protection by design requirement of the GDPR in a report of the European Parliament.[[13]](#footnote-13) Nonetheless difficulties remain regarding little research has been done on this cryptographic process resulting in insufficient trust, as well as the danger of decryption in case of a cryptoanalytic success[[14]](#footnote-14) Since transactional data is not pseudonym, but anonym it is questionable if Zcash even falls under the scope of the GDPR. Transactional data is as discussed above not the only data that qualifies to be personal. Nonetheless Zcash is a global network that uses IP addresses to maintain connections between nodes.[[15]](#footnote-15) IP addresses (meta data) cannot identify a person directly but can indirectly because with IP addresses precise conclusion can be drawn regarding the private life of a person.[[16]](#footnote-16) It is therefore data that can only be attributed while using additional information, which is pseudonym and thus personal data under the GDPR.[[17]](#footnote-17)

* 1. Legal grounds for data processing

Because of their decentralized structure blockchains enable a new way to ensure untrusted parties to collaborate, without having a central intermediary. The goal of cryptocurrencies is instead of solving economic exchange and social coordination problems with centralized institutions (such as banks), to solve them solemnly with technical means. [[18]](#footnote-18) But this collaboration involves processing of personal data in terms of the GDPR, since transactional data is pseudonym and therefore qualifies as personal data.[[19]](#footnote-19) Processing of personal data however can only be lawful under the GDPR, where it is permitted through a legal ground. In accordance with Article 4(7) GDPR this implementation falls into the scope of duty of the data controller. Because cryptocurrencies are decentralized and designed to be operated by many parties the qualification of (joint-) data controllers are difficult and needs to be determined on a case-by-case basis.[[20]](#footnote-20) The perception of the data controller includes three requirements: a natural or legal person (entity), a pluralist liability and lastly[[21]](#footnote-21), the entity needs to be able to determine the purpose and means of the personal data processing.[[22]](#footnote-22)

In general, the decision which software, hardware, and data center to use for public permissionless blockchain is made by a range of different actors and not by one legal entity. As a first step to clarify who can be qualified as a data controller for public permissionless blockchain the different stakeholders of Zcash will be examined.

* 1. Stakeholders

Stakeholders in blockchain projects rely mostly on their inherent technological regulations. Public permissionless blockchains rely on several formally independent participants to maintain and run the system. Simultaneously every stakeholder might have different interest regarding the system, which may result in in different expectations about how such a system should run or even be built. The importance of common grounds is especially relevant in blockchain technologies, because if missing, a blockchain forks technically and organizationally.[[23]](#footnote-23) To identify stakeholders in cryptocurrencies not only the blockchain governance needs to be considered, but also complementors, governments, banks, institutions, companies, and affiliations.

Because stakeholders have different interests, cryptocurrency projects also have different focuses in their design. These design features can for example be anonymity, data security or integrity.[[24]](#footnote-24) Zcash set their focus on privacy and thus provides higher transaction anonymity and privacy than other cryptocurrencies.[[25]](#footnote-25) Regarding data processing in a blockchain environment, different stakeholders may be singled out: nodes and miners, users interacting with blockchains by means of wallets or other front-end services and lastly application operators processing data to and from the blockchain when providing services by means of application. Since the justification for personal data processing must be done by the data controller, it also needs to be determined which stakeholders qualify to be data controller.[[26]](#footnote-26)

Miners or Nodes analyze the consensus according to the protocol as it is defined in the blockchain software, but they do not decide what kind of data is written to the blockchain in a fully decentralized network. The technology of blockchain is exactly designed, that miners and nodes cannot control the content of a blockchain. Instead of being considered data controller they can be viewed as infrastructure. This way the problem of necessary documentation under the GDPR does not arise.[[27]](#footnote-27)

Wallets allow companies or individuals to control their own private key and allow interaction with the blockchain network, by sending transactions to the miners for processing. Wallets are software packages at the application level and may pass personal data to miners. Data is only passed if directed by the user of Zcash, thus he/she is in control of processing the personal data or application, which might be operated by a central institution which can be seen as a data processor.[[28]](#footnote-28)

Developers of blockchain protocols do not process or collect data, but create tools, which can be used by other participants in the system and define this way how data is processed.[[29]](#footnote-29) But with the publication of the code, developers give up control over it.[[30]](#footnote-30) Taking this into consideration developers of blockchain protocols should not be considered data controller.[[31]](#footnote-31) This might not be the case in case of Zcash, since founders own more than 10% of all coins.[[32]](#footnote-32) It is also to be examined if therefore the founders of Zcash as a legal entity can be considered potential data controllers. If a legal entity can determine the purpose and means of the personal data processing it is viewed as a data controller.[[33]](#footnote-33) The first requirement is that the founders need to be an entity, the founders of Zcash could be considered joint-controllers.[[34]](#footnote-34) As seen in a Court decision in the Jehovan Witnesses case, the religious community can regarding the preaching be considered data controllers[[35]](#footnote-35) The term is broadly interpreted and founders of Zcash are likely to qualify as data controllers regarding this requirement. As an entity that already developed the project and holds over 10% of all coins, they have more control over the purpose of data processing than other users. They exert influence over data processing since they chose, used hardware and software. In addition, the decentralization in Zcash is put into question and the decision making is not truly distributed because founders hold a significant number of coins. Even though founders normally should not qualify as data controllers, in the case of Zcash a qualification should be considered.

* 1. Legal grounds

Article 6 GDPR states an exhaustive list of different grounds which justify data processing. Consent being the first to provide a possible legal ground. It has been suggested that it would provide justification in accordance with Article 6 GDPR, but this application comes with two problems. On one hand the GDPR included the right to ‘withdraw his or her consent at any time’, but the personal data is if once included to the blockchain, processed as long as the ledger exists.[[36]](#footnote-36) On the other hand, consent is only provided 'by a clear affirmative actestablishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data'[[37]](#footnote-37) in accordance with the Regulation. Consent according to Article 6(1) cannot be given in DLTs and is not a suitable legal ground for legal data processing. Possible legal grounds are however Article 6(1) GDPR where the existing contractual agreement between parties can also built the legal justification for the use of DLT for related personal data processing. Personal data processing is also lawful where it is needed for ‘compliance with a legal obligation to which the controller is subject’[[38]](#footnote-38), in context with Zcash this may be from importance for transaction that require compliance with Know Your Customer and Anti-Money Laundering or if personal data is required to comply with tax law.[[39]](#footnote-39) But also the Stakeholder who provide services (for example banks) have consent as legal grounds for personal data processing. Because if banks use Zcash to execute their contractual obligation towards a client, they have a contract according to article 6(2) GDPR.

Unlikely to be of relevance for data processing for public permissionless blockchain and therefore Zcash are however ‘the protection of the vital interests of the data subject or another natural person’[[40]](#footnote-40) and ‘carrying out a task in the public interest or the exercise of official authority’.[[41]](#footnote-41)

Lastly processing can occur where it is necessary for legitimate interests. It can be necessary from the view of a third party or the data controller. It can be used whether a contractual relationship exists or not, it is a flexible ground and enjoys general nature. However, the application in real life is difficult because the definition of legitimate interests is not always clear. According to the preamble of the GDPR personal data processing for direct market processing can be following a legitimate interest.

In conclusion data processing is most likely to be justified through existing contractual agreements, compliance reasoning with the KYC and AML, and consent.

1. Implementation of Data Subject Rights in Blockchains

*Written by Lynn Grau*

The past view years a set of problems have risen between the GDPR and blockchain technologies some have already been discussed above while others will be examined hereinafter. These tensions can be said to be rooted in two main characteristics of the GDPR. First the new data protection law is first and foremost made for data processing in central systems, meaning it is defined by the idea that the accountability and responsibility rests with the data controller.[[42]](#footnote-42) DLT is by its nature decentralized and therefore does not have a legal or natural person who data subjects can address to enforce their rights and therefore it is difficult to determine who’s responsible.[[43]](#footnote-43) Because the data subject rights in the articles 15 to 22 GDPR are to be exercised through the data controller. Some of said rights may not raise tensions with the GDPR, the others will be examined in the following.

Articles 15 GDPR foresees the right to demand disclosure to what kind of data and for what reason it is processed and where it comes from. In public permissionless blockchain the implementation of this right is once again problematic because a clear qualification of a data controller is missing. Taking the transparency into consideration, this right can be met because the data on the blockchain is public for the user. In this paper this opinion is followed, and the right is met.[[44]](#footnote-44)

According to article 17 GDPR consent for data processing should be as easily withdrawn as user can grant it, meaning it lays down the right for data subjects to have their personal data erased, if it is held without a legal ground to retain or process it.[[45]](#footnote-45) Personal data must be removeable if it is held without a legal basis[[46]](#footnote-46), but contradicting the GDPR personal data is saved on a ledger in a permanent and tamper-proof way. The right to be forgotten opposes the fundamental technology of public permissionless blockchains, because it would negate irreversibility/immutability, one of the main principles of a blockchains architecture. Data under the GDPR is accurate if it appropriately recalls a fact in connection with the data subject regarding a purpose.[[47]](#footnote-47) If inaccurate, the person is entitled to demand rectification of said data.[[48]](#footnote-48) This right raises tensions because of the same reason as discussed above, regarding ‘the right to be forgotten’.[[49]](#footnote-49)

Zcash being a public permissionless blockchain also faces this problem. Because of the decentralized and concatenated structure of the blockchain a post hoc rectification or erasure is complicated or even impossible.

According to Zcash, this privacy protecting currency is especially well positioned to support the legal requirements of the regulation. Taking a closer look at transactions out of 2,242,847 transactions made across all blocks of Zcash only 14.6% are private transactions, meaning both parties used z-shielded addresses. Thus, a major part of the activities on Zcash do not use shielded addresses. Since Zcash is a (code) fork of Bitcoin, t-address transactions are identical to this prominent cryptocurrency and can be deanonymized as well.[[50]](#footnote-50) The users may consent to share their transactional data with select third parties within Zcash to ensure compliance with the GDPR regarding the right for ‘privacy by design’.

1. Anticipated Problems with public permissionless Blockchains regarding the revADP

*Written by Lynn Grau*

The revised Swiss Data Protection Act is very similar to the GDPR. The guiding principle for both acts was the Convention 108+ of the Council of Europe and the Police and Justice Directive of the EU. Switzerland ratified the Con 108+ in 1997 and the revised version will be as well. Therefore, the Con 108+ is binding for Switzerland and was the fundamental principle while revising the ADP. Even though the revADP and the GDPR exhibit many similarities, there are still some differences.[[51]](#footnote-51) Since the GDPR and the revADP are very alike, similar problems regarding public permissionless blockchain are to be anticipated. Both regulations are designed for centralized systems and thus Zcash (public permissionless blockchain in general) are at odds with the Swiss Regulation. The revADP has extended the rights of data subjects through rewording and the implementation of the right to data portability. The extension of consequences resulting in this right are hard to determine, since this term has been copied from the GDPR and a jurisdiction does not exist yet.[[52]](#footnote-52) However, the data subject rights in the revADP are still not as extensive as they are in the GDPR. ‘The right to erasure’[[53]](#footnote-53) and ‘the right of rectification’[[54]](#footnote-54) aren’t rights data subjects can address under the revADP. They are as examined above a tension point between the GDPR and Zcash regarding compliance, the revADP is in this aspect more DLT friendly.

These arguments lead to the conclusion that public permissionless blockchain for example Zcash are going to raise tensions when the revADP enters into force in 2023. Considering that it is not as extensive as the GDPR, there will however be fewer problems. The exact effect of the revADP on public permissionless blockchains can only be made if the act has been implemented and jurisdiction regarding blockchains exist.

1. Conclusion

The tensions between blockchain technology and European data protection regulations, namely the GDPR and the revADP, remain even four years after the GDPR has been put into force. However general assumptions cannot be made because cryptocurrencies differ in the cryptographic methods they employ, as seen in chapter 2.1. Even in privacy coins you can theoretically link transactions to users, hence they are not fully anonymous. Thus, data processed on blockchains is partly pseudonym and qualifies as personal data under the GDPR. Although the privacy they provide is indisputably higher they fall under the same category and under the scope of the regulation. To define the exact problems regarding the compatibility of the GDPR or revADP and a blockchain project a case-by-case analysis needs to be assessed instead of grouping all cryptocurrencies under the same laws. This is especially from importance, with cryptocurrencies that use technical solutions to comply with the GDPR. As seen with Zcash, the privacy feature in this blockchain solves only certain problems regarding the GDPR and the revADP, tensions remain, and it is not completely private.

Although privacy seems to be weaker in bitcoin it all depends on how the user acts. In all cryptocurrencies a user can somehow state and prove that they were behind a transaction, thus making it impossible to be fully anonymous. However, the announcement does not happen on the blockchain itself. It happens on other platforms. UTXO based blockchains have no means of deanonymizing a person themselves.

Declaration of Authorship

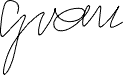
„Ich erkläre hiermit, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Mir ist bekannt, dass andernfalls die Arbeit mit der Note 1 bewertet wird und der Senat gemäss Artikel 36 Absatz 1 Buchstabe r des Gesetzes über die Universität vom 5. September n 1996 und Artikel 69 des Statuts der Universität Bern vom 7. Juni 2011 zum Entzug des aufgrund dieser Arbeit verliehenen Titels berechtigt ist.

Für die Zwecke der Begutachtung und der Überprüfung der Einhaltung der Selbständigkeitserklärung bzw. der Reglemente betreffend Plagiate erteile ich der Universität Bern das Recht, die dazu erforderlichen Personendaten zu bearbeiten und Nutzungshandlungen vorzunehmen, insbesondere die schriftliche Arbeit zu vervielfältigen und dauerhaft in einer Datenbank zu speichern sowie diese zur Überprüfung von Arbeiten Dritter zu verwenden oder hierzu zur Verfügung zu stellen.“

Ort, Datum Eigenhändige Unterschrift



Bern, 22.4.2022



1. S. Nakamoto, „Bitcoin whitepaper,“ *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019),* p. 6, 2008. [↑](#footnote-ref-1)
2. Ben Wolford: What is GDPR, the EU’s new data protection law? < <https://gdpr.eu/what-is-gdpr/>> (last recall on 20.04.2022). [↑](#footnote-ref-2)
3. EPRS study, p. II. [↑](#footnote-ref-3)
4. EPRS study, p. 7. [↑](#footnote-ref-4)
5. Sorge, p. 14. [↑](#footnote-ref-5)
6. EPRS study, p. 15. [↑](#footnote-ref-6)
7. EPRS Study, p 15. [↑](#footnote-ref-7)
8. EPRS Study, p 28. [↑](#footnote-ref-8)
9. X. Sun, F. R. Yu/P. Zhang/Z. Sun, W. Xie/X. Peng: "A Survey on Zero-Knowledge Proof in Blockchain," in IEEE Network, vol. 35, no. 4, pp. 198-205, July/August 2021, doi: 10.1109/MNET.011.2000473. p. 198. [↑](#footnote-ref-9)
10. EPRS [↑](#footnote-ref-10)
11. Chapter 2.1.2 B [↑](#footnote-ref-11)
12. Plattner, p. [↑](#footnote-ref-12)
13. European Parliament (27 November 2018) Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018) para 21. [↑](#footnote-ref-13)
14. Plattner, p.15. [↑](#footnote-ref-14)
15. Privacy Recommendations and Best Practices: < <https://z.cash/support/security/privacy-security-recommendations/>>. (last recalled on 20.4.22) [↑](#footnote-ref-15)
16. EPRS, p. 16. [↑](#footnote-ref-16)
17. Article 4(5) GDPR. [↑](#footnote-ref-17)
18. Schmid/Ziolkowski/Schwabe, p. 6093. [↑](#footnote-ref-18)
19. Article 4(5) GDPR, [↑](#footnote-ref-19)
20. EPRS study, p. 42. [↑](#footnote-ref-20)
21. Jaccard Gabriel/Tharin Adrien: GDPR & Blockchain: the Swiss take, in: Jusletter IT 4. December 2018, p. 11. [↑](#footnote-ref-21)
22. Article 4(7), GDPR. [↑](#footnote-ref-22)
23. Schmid/Ziolkowski/Schwabe, p. 6098. [↑](#footnote-ref-23)
24. Schmid/Ziolkowski/Schwabe, p. 6098. [↑](#footnote-ref-24)
25. The Basics: < <https://z.cash/the-basics/>>. (last recalled 20.4.22) [↑](#footnote-ref-25)
26. Eichler/ Jongerius/McMullen/ Naegele/Steininger/ Wagner, p. 5. [↑](#footnote-ref-26)
27. Eichler/ Jongerius/McMullen/ Naegele/Steininger/ Wagner, p. 6. [↑](#footnote-ref-27)
28. Eichler/ Jongerius/McMullen/ Naegele/Steininger/ Wagner, p. 6. [↑](#footnote-ref-28)
29. Eichler/ Jongerius/McMullen/ Naegele/Steininger/ Wagner, p. 6. [↑](#footnote-ref-29)
30. Plattner, p. . [↑](#footnote-ref-30)
31. Eichler/ Jongerius/McMullen/ Naegele/Steininger/ Wagner, p. 6. [↑](#footnote-ref-31)
32. 2,1.2 b [↑](#footnote-ref-32)
33. Article 4(7), GDPR. [↑](#footnote-ref-33)
34. Article 26, GDPR. [↑](#footnote-ref-34)
35. Case C-25/17 *Jehovan todistajat* [2018] EU:C:2018:551. [↑](#footnote-ref-35)
36. EPRS study, p. 60. [↑](#footnote-ref-36)
37. Article 32, GDPR. [↑](#footnote-ref-37)
38. Article 6(1)c GDPR. [↑](#footnote-ref-38)
39. EPRS study, p. 62. [↑](#footnote-ref-39)
40. Article 6(1)d GDPR. [↑](#footnote-ref-40)
41. Article 6(1)e GDPR. [↑](#footnote-ref-41)
42. EPRS study, p. II. [↑](#footnote-ref-42)
43. Tatar/Gokce/ Nussbaum, p. 6. [↑](#footnote-ref-43)
44. Plattner, p. 48. [↑](#footnote-ref-44)
45. Tatar/Gokce/ Nussbaum, p. 4. [↑](#footnote-ref-45)
46. If special categories of data are being processed, different principles may apply. [↑](#footnote-ref-46)
47. Plattner, p. 49. [↑](#footnote-ref-47)
48. Article 15 GDPR [↑](#footnote-ref-48)
49. Plattner, p. 50 [↑](#footnote-ref-49)
50. Kappos/Yousaf/Maller/Meiklejohn, p. 466 [↑](#footnote-ref-50)
51. Baeriswyl, p. 9. [↑](#footnote-ref-51)
52. Baeriswyl, p. 14. [↑](#footnote-ref-52)
53. Article 17, GDPR [↑](#footnote-ref-53)
54. Article 16, GDPR [↑](#footnote-ref-54)