Universität Bern

Rechtswissenschaftliche Fakultät

How can Privacy considerations be consolidated with transaction transparency?

Computer Science and Private Law

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

Einreichungsdatum: 22. April 2022

Verfassende: Marius Asadauskas, Lynn Grau

Adresse: Murtenstrasse 143e, 3008 Bern

Sulgenheimweg 17, 3007 Bern

Matrikelnummer: 11-111-111, 18-629-

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

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

Inhaltsverzeichnis

[Literaturverzeichnis IV](#_Toc101382108)

[Materialienverzeichnis VI](#_Toc101382109)

[Abkürzungsverzeichnis VII](#_Toc101382110)

[1 Introduction 1](#_Toc101382111)

[1.1 Personal, anonymous and pseudoanonymised data 1](#_Toc101382112)

[1.2 GDPR basics 1](#_Toc101382113)

[1.3 UTXO vs Account Based Blockchains 1](#_Toc101382114)

[2 Related Works 1](#_Toc101382115)

[2.1 UTXO vs Account Based Blockchains 1](#_Toc101382116)

[2.2 Different Cryptocurrencies 1](#_Toc101382117)

[2.2.1 Bitcoin 1](#_Toc101382118)

[2.2.2 Ethereum 1](#_Toc101382119)

[2.2.3 Privacy Coins 1](#_Toc101382120)

[A Monero 1](#_Toc101382121)

[B Dash 1](#_Toc101382122)

[2.2.4 Metamask 1](#_Toc101382123)

[3 Privacy and the Law in Europe 2](#_Toc101382124)

[3.1 Data Privacy Regulations and public permissionless Blockchains 2](#_Toc101382125)

[4 Tensions between the GDPR and public permissionless Blockchains 3](#_Toc101382126)

[4.1 Legal grounds for data processing 5](#_Toc101382127)

[4.2 Stakeholders 5](#_Toc101382128)

[4.3 Conclusion 8](#_Toc101382129)

[4.4 Other Problems between the GDPR and public permissionless Blockchains 8](#_Toc101382130)

[4.5 Anticipated Problems with public permissionless Blockchains regarding revDPA 10](#_Toc101382131)

[5 Conclusion 11](#_Toc101382132)

[Selbständigkeitserklärung 12](#_Toc101382133)

Bibliography

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>.

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.

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>

European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), Briefing, STOA Options Brief, 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/EP RS\_STU(2019)634445(ANN1)\_EN.pdf>.

Schmid Roman/Ziolkowski Rafael/ Schwabe Gerhard: Together or Not? Explorng 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>.

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>.

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>.

X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie and 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

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

List of abbreviations

BC Blockchain

GDPR General Data Protection Regulation

revDPA revised Swiss Data Protection Act

DLT Distributed Ledger Technology

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

Introduction

The first blockchain network was the cryptocurrency Bitcoin launched in 2009. Since then, blockchain technology has gained a lot of popularity. The growth of DLT over the last decade has let to the recognition of the underlying technology potential of BC 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.

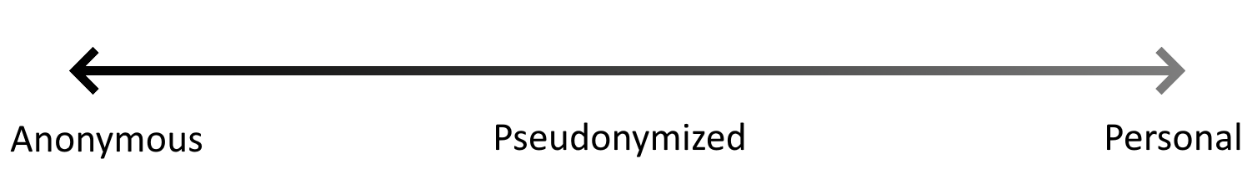
* 1. Personal, anonymous and pseudonymized data

*Written by Marius Asadauskas*

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 a person’s medical records.

After personal data there is pseudonymized data. This is information, that can be linked through indirect means to a natural person, such as Satoshi Nakamoto using a pseudonym while developing bitcoin. If we were to link the pseudonym to an identity, we would find out a lot of personal data about that person. Data which cannot be linked to a person through any means is anonymous data and is outside of most laws. [[1]](#footnote-1)

The scale of anonymous data 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

UTXO stands for unspent transaction output. Bitcoin was the first cryptocurrency to implement transactions based on UTXO’s. For each transaction output a utxo is made and given to the receiver. The receiver can later use any combination of UTXO’s inside other transactions. You can imagine this as a paper bill with the currency written on it.

On the other hand, account-based transactions have addresses and balances. When you transfer money to someone your balance decreases and theirs increases. This simplifies the transaction process but creates 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 however leak a public key in an account-based cryptocurrency, you leak all your transactions.

1. Privacy in Distributed Ledgers
   1. Different Cryptocurrencies

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 that possibility. They must be accessible to everyone, and no data can be hidden. What instead can be hidden is the information held by the data. This is done through cryptographic means. Notable cryptographic methods include the use of public and private keys, zero knowledge proofs, optimistic proofs, 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[[2]](#footnote-2). Instead of using personal data such as one’s name, address, and birthday to make a transaction, bitcoin uses public and private keys to receive and create transactions.

An example of how bitcoin is not anonymous would be the fact that 1.1 million bitcoins have been linked to Satoshi Nakamoto[[3]](#footnote-3). Although all the best privacy measures were used, we still now 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, it is obvious how this would be personal information.

The method used in the mentioned report cannot be applied to every person but if anyone ever leaks their public keys, all transactions done with those keys become linkable to that person.

Considering the right to be forgotten[[4]](#footnote-4) the permanent and public nature of bitcoin is (in direct violation of this law).

**Address Reuse**

It is possible to only use one address forever but that would be against all recommendations. In conclusion bitcoin is as private as you make it, so if you employ good practices and never reuse wallet addresses and never leak your own information it will be very close to anonymous but if you do not follow these principles, it will quickly become pseudonymous.

**Bitcoin Mixers**

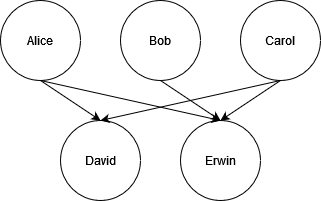
A way to further increase privacy in the bitcoin network is to use other services provided there.

* + 1. Privacy Coins

Privacy coins are cryptocurrencies which hide transaction details from the public[[5]](#footnote-5). Privacy coins are usually more computationally heavy, require more storage space and are more complex in general, but these downsides are outweighed by the privacy they provide.

* + - 1. Monero

Monero uses ring signatures to hide transactions[[6]](#footnote-6). You are forced to use one-time keys as reusing a public key more than once causes rings to be linked and the transaction to be marked as invalid. This stops double spending attacks and also increases privacy.



You can see that both David and Erwin receive money, but who exactly send them the money is unknown, since each transaction requires multiple utxo’s as inputs.

* + - 1. Z-Cash

Z-cash

Is split up into two address types of transparent t-addresses and private z-addresses. It follows that four types of transactions can happen in the z-cash network. T-t

Z-cash uses a cryptographic method known as zero knowledge proofs, in which you prove you know a secret without sharing the secret.

A simple example of a zero-knowledge proof would be Alice proving to Bob that she knows the code to a safe. Alice could show the safe being closed, then secretly enter the code, and show it being open to Bob. This way Alice has proven that she knows the safe combination without revealing it to Bob.

In the case of Z-cash however this is done with complex mathematics.

It is important to note that the founders own 2.1 million coins with there being a maximum of 21 million coins. They hold more than 10% of the z-cash market, which puts the distributed nature of the ledger into question.

1. Privacy and Data Protecting Law in Europe

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.[[7]](#footnote-7) Violations and non-compliance results in harsh fines, with penalties that can reach tens of millions of euros. The revised DPA is as the GDPR a data protection acts who aims to protect the privacy of natural people.

* 1. Data Privacy Regulations and public permissionless Blockchains

Many blockchains are at odds with these legal requirements. But there isn’t the one BC, 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, BC illustrate a class of technology, that contains many versions, who differ in complexity and their technical and governance arrangement. Therefore, it can’t be concluded if BCs in general are compatible with the GDPR or the revDPA, but a case-by-case analysis is to be assessed. However, it is harder to design a public permissionless BC, because they lack control over which actors have access to the relevant data and don’t have control over the network to treat data in a compliant manner. Hereinafter the compatibility between the data protection acts and public permissionless BC 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 2.2.4) will be used as an example.

1. Tensions between the GDPR and public permissionless Blockchains

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 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.[[8]](#footnote-8) 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. 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.[[9]](#footnote-9) Other categories of data that aren’t public keys but may be used on blockchains are transactional data, such as name or address that is 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.

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, which is an interactive verification protocol.[[10]](#footnote-10) A person can proof a binary True/False statement, without having to provide access to the underlying data,[[11]](#footnote-11) if both parties use z-addresses.[[12]](#footnote-12) 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 doesn’t process identifiable information, because it eliminates the need to track data through the transaction process. Zcash enable with Zero-Knowledge-Proofs fully anonymized transactions on the BC.[[13]](#footnote-13) Sk-SNARKs have the potential to facilitate compliance with article 26 GDPR the right for ‘data protection by design’.[[14]](#footnote-14) Zk-SNARKs have been considered to be compliant with the data protection by design requirement of the GDPR in a report of the European Parliament.[[15]](#footnote-15) 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.[[16]](#footnote-16) 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.[[17]](#footnote-17) IP addresses (meta data) can’t identify a person directly but can indirectly because with IP addresses precise conclusion can be drawn regarding the private life of a person. It is therefore data that can only be attributed while using additional information, which is pseudonym and thus personal data under the GDPR.[[18]](#footnote-18)

* 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. [[19]](#footnote-19) But this collaboration involves processing of personal data in terms of the GDPR, since transactional data is pseudonym and therefore qualifies as personal data.[[20]](#footnote-20) 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 is difficult and needs to be determined on a case-by-case basis.[[21]](#footnote-21) In general the decision which software, hardware, and data center to use for public permissionless BC 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 BC 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, they fork technically and organizationally.[[22]](#footnote-22) 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.[[23]](#footnote-23) Zcash set their focus on privacy and thus provides higher transaction anonymity and privacy than other cryptocurrencies.[[24]](#footnote-24) 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.

Miners or Nodes analyze the consensus according to the protocol as it is defined in the blockchain software, but they don’t decide what kind of data is written to the blockchain in a fully decentralized network. The technology of BC is exactly designed that miners and nodes cannot control the content of a BC.[[25]](#footnote-25) Instead of being considered data controller they can be viewed as infrastructure. This way the problem of necessary documentation under the GDPR doesn’t arise. However, the decentralization is put into questions in Zcash, since founders own more than 10% of all coins.[[26]](#footnote-26) It is to be examined if therefore the founders of Zcash as a legal entity can be considered potential data controllers.

Wallets allow companies or individuals to control their own private key and allow interaction with the BC 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.

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.[[27]](#footnote-27) But with the publication of the code, developers give up control over it.[[28]](#footnote-28) Taking this into consideration developers of blockchain protocols should not be considered data processors.[[29]](#footnote-29)

* 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. 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' in accordance with the Regulation. Content 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’[[30]](#footnote-30), 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.[[31]](#footnote-31) 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).

Unlikely to be of relevance for data processing for public permissionless BC and therefore Zcash are however ‘the protection of the vital interests of the data subject or another natural person’[[32]](#footnote-32) and ‘carrying out a task in the public interest or the exercise of official authority’.[[33]](#footnote-33)

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.

* 1. Other Problems between the GDPR and public permissionless Blockchains

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.[[34]](#footnote-34) DLT is by its nature decentralized and therefore doesn’t 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.[[35]](#footnote-35) 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 BC 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.[[36]](#footnote-36)

According to article 17 EU 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.[[37]](#footnote-37) Personal data must be removeable if it is held without a legal basis[[38]](#footnote-38), 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. Because of the decentralized and concatenated structure of BC a post hoc rectification or erasure is complicated or even impossible. If inaccurate, the person is entitled to demand rectification of said data.[[39]](#footnote-39) This right raises tensions because of the same reason as discussed above, regarding the right to be forgotten.[[40]](#footnote-40)

Zcash being a public permissionless blockchain also faces this problem. Because of the decentralized and concatenated structure of the BC 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, because it doesn’t fall under the scope of the GDPR. Taking a closer look at transactions however 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.[[41]](#footnote-41) 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 revDPA

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 DPA. Even though the revDPA and the GDPR exhibit many similarities, there are still some differences.[[42]](#footnote-42) Since the GDPR and the revDPA are very alike, similar problems regarding public permissionless BC are to be anticipated. Both regulations are designed for centralized systems and thus Zcash (public permissionless BC in general) are at odds with the Swiss Regulation because. The revDPA 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. However, the data subject rights in the revDPA are still not as extensive as they are in the GDPR.[[43]](#footnote-43) ‘The right to erasure’[[44]](#footnote-44) and ‘the right of rectification’[[45]](#footnote-45) aren’t rights data subjects can address under the revDPA. They are as examined above a tension point between the GDPR and Zcash regarding compliance, the revDPA is in this aspect more DLT friendly.

1. Conclusion

Selbständigkeitserklärung

„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

1. Art. 4 GDPR, Definition: https://gdpr-info.eu/art-4-gdpr/ [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/ [↑](#footnote-ref-3)
4. Art. 17 GDPR [↑](#footnote-ref-4)
5. [↑](#footnote-ref-5)
6. [↑](#footnote-ref-6)
7. *Finck*, Blockchain and the General Data Protection Regulation, S. 32; *Finck*, Blockchains and Data Protection in the EU, S. I. f. <https://ssrn.com/abstract=3080322> (zuletzt abgerufen am 29.03.2022). [↑](#footnote-ref-7)
8. SORGE CHRISTOPH, p. 14 [↑](#footnote-ref-8)
9. EPRS Study, p. [↑](#footnote-ref-9)
10. X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie and X. Peng, p. 198 [↑](#footnote-ref-10)
11. EPRS [↑](#footnote-ref-11)
12. 2.1.2 B [↑](#footnote-ref-12)
13. PLATTNER MATTHIAS, p. [↑](#footnote-ref-13)
14. European Parliament (27 November 2018) Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018) para 21. [↑](#footnote-ref-14)
15. European Parliament (27 November 2018) Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018) para 21. [↑](#footnote-ref-15)
16. PLATTNER MATTHIAS, p. [↑](#footnote-ref-16)
17. Z.cash.com [↑](#footnote-ref-17)
18. Article 4(5) GDPR [↑](#footnote-ref-18)
19. Together or not? Exploring Stakeholder in Public Permissionless Blockchains. [↑](#footnote-ref-19)
20. Article 4(5) GDPR [↑](#footnote-ref-20)
21. EPRS study, p. 42 [↑](#footnote-ref-21)
22. Together or not? Exploring Stakeholder in Public Permissionless Blockchains. [↑](#footnote-ref-22)
23. 6098 [↑](#footnote-ref-23)
24. Z.cash.ch [↑](#footnote-ref-24)
25. PLATTNER MATTHIAS,. [↑](#footnote-ref-25)
26. 2,1.2 b [↑](#footnote-ref-26)
27. Natalie Eichler, Silvan Jongerius, Greg McMullen, Oliver Naegele, Liz Steininger, Kai Wagner: Blockchain, data protection and the GDPR, S. 6 [↑](#footnote-ref-27)
28. PLATTNER MATTHIAS, Datenschutzrechtliche Herausforderungen der Distributed-Ledger-Tech- nologie, Rechtliche Fragestellungen, Zürich 2021, p. 35-59, available under: <https:// www.swisslex.ch/de/doc/bookdoc/a96ab058-ab8f-49a3-a96f-b2b0d47a3266>. [↑](#footnote-ref-28)
29. Natalie Eichler, Silvan Jongerius, Greg McMullen, Oliver Naegele, Liz Steininger, Kai Wagner: Blockchain, data protection and the GDPR, S. 6 [↑](#footnote-ref-29)
30. Article 6(1)c GDPR [↑](#footnote-ref-30)
31. STOA p. 62 [↑](#footnote-ref-31)
32. Article 6(1)d GDPR [↑](#footnote-ref-32)
33. Article 6(1)e GDPR [↑](#footnote-ref-33)
34. The law of crypto assets [↑](#footnote-ref-34)
35. Tatar Unal/Gokce Yasir/ Nussbaum Brian:, S. 6 [↑](#footnote-ref-35)
36. Plattner, p. 48 [↑](#footnote-ref-36)
37. Tatar Unal/Gokce Yasir/ Nussbaum Brian [↑](#footnote-ref-37)
38. If special categories of data are being processed, different principles may apply. [↑](#footnote-ref-38)
39. Article 15 GDPR [↑](#footnote-ref-39)
40. Plattner, p. 50 [↑](#footnote-ref-40)
41. Kappos/Yousaf/Maller/Meiklejohn, p. 466 [↑](#footnote-ref-41)
42. Baeriswyl, p. 9. [↑](#footnote-ref-42)
43. [↑](#footnote-ref-43)
44. Article 17 GDPR [↑](#footnote-ref-44)
45. Article 16 GDPR [↑](#footnote-ref-45)