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: 18-106-575, 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 III](#_Toc101441145)

[Materialienverzeichnis IV](#_Toc101441146)

[Abkürzungsverzeichnis V](#_Toc101441147)

[1 Introduction 1](#_Toc101441148)

[1.1 Personal, anonymous and pseudonymized data 1](#_Toc101441149)

[1.2 UTXO vs Account Based Blockchains 1](#_Toc101441150)

[2 Privacy in Distributed Ledgers 2](#_Toc101441151)

[2.1 Different Cryptocurrencies 2](#_Toc101441152)

[2.1.1 Bitcoin 3](#_Toc101441153)

[A Address Reuse 3](#_Toc101441154)

[B Bitcoin Mixers 4](#_Toc101441155)

[C Violating your own privacy 4](#_Toc101441156)

[2.1.2 Privacy Coins 4](#_Toc101441157)

[2.1.3 Monero 5](#_Toc101441158)

[A Violating your own privacy 6](#_Toc101441159)

[2.1.4 Z-Cash 6](#_Toc101441160)

[3 Legal Ramifications 7](#_Toc101441161)

[4 Conclusion 7](#_Toc101441162)

[Selbständigkeitserklärung 8](#_Toc101441163)

Literaturverzeichnis

Emmenegger Susan/Tschentscher Axel: Art. 1, in: Heinz Hausheer/Hans Peter Walter (Hrsg.), Berner Kommentar. Kommentar zum schweizerischen Zivilgesetzbuch, Bd. I Einleitung und Personenrecht, 1. Abteilung Einleitung Artikel 1-9 ZGB, Bern 2012, S. 131-431.

Kunz Karl-Ludwig/Mona Martino: Rechtsphilosophie, Rechtstheorie, Rechtssoziologie. Eine Einführung in die theoretischen Grundlagen der Rechtswissenschaft, Bern u.a. 2006.

Müller Markus: Individuelle Selbstbestimmung und staatliche Fürsorge, ZSR 131 (2012) I, S. 63-86.

Materialienverzeichnis

Botschaft vom 8. Juni 2012 zur Änderung des Bundegesetzes über die Zusammenarbeit mit den internationalen Gerichten zur Verfolg schwerwiegender Verletzung des humanitären Völkerrechts, BBl 2012 6663 (nachfolgend zitiert: Botschaft internationale Gerichte)

Eidgenössisches Justiz- und Polizeidepartement, Erläuternder Bericht zur Verordnung über Kaltwasserzähler, 3. Mai 2012

Empfehlungen der Schweizerischen Akademie der Medizinischen Wissenschaften (SAMW) vom 29. Mai 2012 betreffend die ethische Unterstützung in der Medizin (http://www.samw.ch)

Bundesamt für Justiz, Zutrittskontrollen in Stadien: Durchsuchungen im Intimbereich, Gutachten vom 3. Februar 2011, VPB 2012.2 S. 18-27.

Abkürzungsverzeichnis

EBV [Bernische ] Verordnung vom 24. März 2010 über die Erziehungsberatung, BSG 431.13

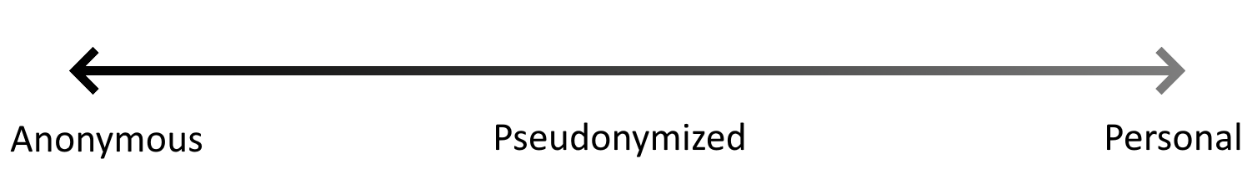
PAG Bundesgesetz vom 20. März 2009 über die Patentanwältinnen und Patentanwälte (Patentanwaltsgesetz, SR 935.62)

1. Introduction
   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 this 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. [1]

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 and the miner gets it.

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 the other persons account address. This allows for you to then transfer any given amount you want. Thus, your balance then decreases and the destination account balance increases. This simplifies transactions and makes it easier to use wallets, collect all your assets in one place, it is easier to implement 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. Notably, it 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 leak a public key in an account-based cryptocurrency, you leak your entire transaction history.

1. Privacy in 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 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 [2]. 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 via RSA encryption [3] to receive and create UTXO’s. The public key acts as a wallet address to which you can send a UTXO and the private key acts as a password to the wallet.

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 the 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 a public key 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 and would remain on the blockchain forever.

Considering the right to be forgotten [5] the permanent and public nature of Bitcoin is in direct violation of this law.

* + 1. Address Reuse

It is possible to only use a single private and public 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 said individual to be known and a leak of their private key would cause all their assets to be in jeopardy. Hence for each transaction you should create a new public and private key pair.

* + 1. Bitcoin Mixers

There are also ways to further increase privacy in the Bitcoin network. A possibility is to employ the use of 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. Another downside is that mixers take fees themselves and increase transaction costs even further.

* + 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 with their private key, we would successfully link a UTXO to an individual. 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 possible owners. To make this possible Monero employs something called ring signatures [8]. In the Bitcoin blockchain 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 actual UTXO. 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 around a 1 in 11 chance of being a part of the transactions where those keys appear.

Furthermore, in the Monero blockchain you are 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 require more computation power and transactions require more storage space, since you have to include multiple public keys. As of 2022 the median Monero transaction takes up 1420 Bytes [10], while the median Bitcoin transaction takes up 224 Bytes [11]. So, the Monero blockchain is hence 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 you.

However, to 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 proves that a 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 used to prove 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 proves 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 something known as zk-SNARKs [12]. Zk-Snarks are used since they are non-interactive and using an interactive proof on a blockchain would be very time and resource consuming.

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.

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

1. Legal Ramifications
2. Conclusion

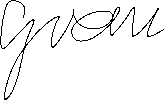
Selbständigkeitserklärung

„Ich erkläre hiermit, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen be-nutzt 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 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

22.04.2022



# Technical Bibliography

|  |  |
| --- | --- |
| [1] | Intersoft Consulting, „Art. 4 Definitions,“ [Online]. Available: https://gdpr-info.eu/art-4-gdpr/. [Zugriff am 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/. [Zugriff am 22 April 2022]. |
| [6] | „Crypto Mixer,“ [Online]. Available: https://cryptomixer.io/. [Zugriff am 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. [Zugriff am 22 April 2022]. |
| [9] | Monero, „Ring Size,“ [Online]. Available: https://www.getmonero.org/resources/moneropedia/ring-size.html. [Zugriff am 22 April 2022]. |
| [10] | Monero, „xmrchain,“ [Online]. Available: https://xmrchain.net/. [Zugriff am 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. |