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 IV](#_Toc98843522)

[Materialienverzeichnis V](#_Toc98843523)

[Abkürzungsverzeichnis VI](#_Toc98843524)

[1 Introduction 1](#_Toc98843525)

[1.1 Personal, anonymous and pseudoanonymised data 2](#_Toc98843526)

[1.2 GDPR basics 2](#_Toc98843527)

[1.3 UTXO vs Account Based Blockchains 2](#_Toc98843528)

[2 Related Works 2](#_Toc98843529)

[2.1 UTXO vs Account Based Blockchains 2](#_Toc98843530)

[2.2 Different Cryptocurrencies 2](#_Toc98843531)

[2.2.1 Bitcoin 2](#_Toc98843532)

[2.2.2 Ethereum 2](#_Toc98843533)

[2.2.3 Privacy Coins 2](#_Toc98843534)

[A Monero 2](#_Toc98843535)

[B Z-Cash 2](#_Toc98843536)

[2.2.4 Metamask 2](#_Toc98843537)

[3 Legal Ramifications 3](#_Toc98843538)

[4 Conclusion 3](#_Toc98843539)

[Selbständigkeitserklärung 4](#_Toc98843540)

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

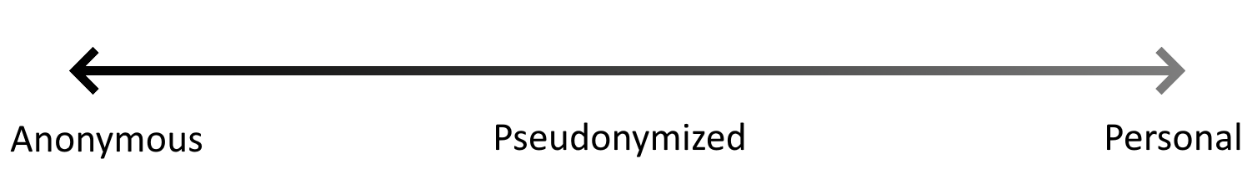
PAG Bundesgesetz vom 20. März 2009 über die Patentanwältinnen und Patentanwälte (Patentanwaltsgesetz, SR 935.62)

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 a person’s unedited medical records.

After personal data there is pseudonymized data. This is information, that can be linked through indirect means to a natural person. An example related to bitcoin would be its creator, Satoshi Nakamoto, using a pseudonym while developing bitcoin. If we were to link the pseudonym to an identity, we would find out lots of personal data about that individual. Data which cannot be linked to a person through any means is anonymous data and 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 employ UTXO based transactions. A real-world example of UTXOs would be the use of bank checks. On a bank check you can write any amount but using a check you can either use all the money 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 works 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. In account-based cryptocurrencies each account has an address and a balance. When transferring money, you require the other persons account address and a given amount you want to transfer. 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 in account-based transactions and it allows the saving of storage space. Sadly, it also 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 your entire transaction history.

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 luxury. 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, 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]](#footnote-2). Instead of using personal data such as one’s name, address, and birthday to make a transaction, bitcoin uses public and private key pair made with RSA[[3]](#footnote-3) to receive and create UTXO’s. The public key acts as a wallet address to which you send money and the private key acts as a password to that wallet.

The first example of how Bitcoin is not anonymous is that if you find an individual’s public keys, you find the individuals transactions. With this you can find out how often they send assets, how much they own and what accounts they send money to.

Another 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]](#footnote-4). Although all the best privacy measures were used, we today 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 be very 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[[5]](#footnote-5) 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 mixers. Mixers take many UTXO as input from different people and returns different

**Violating your own privacy**

In cryptocurrencies it is often possible to mathematically prove that a transaction was yours. RSA key pairs work in both directions. Using the public key is a way to safely communicate with the owner of the key, but the owner can also encrypt with the private key and then everyone can decrypt the message with the public key.

Since only the owner has access to the private key, they can encrypt their own name with it and then it is proof that the person managed the transaction.

* + 1. Privacy Coins

Privacy coins are cryptocurrencies which hide transaction details from the public[[6]](#footnote-6). Privacy coins are usually more computationally heavy, require more storage space and are more complex in general, but in return the privacy they provide is higher.

* + - 1. Monero

Transactions on the Monero blockchain are both untraceable and unlinkable. To make this possible Monero employs something called ring signatures[[7]](#footnote-7). When you want to transfer funds on the Monero blockchain you must sign each transaction with at least 11 public keys, with only one public key being your own. An example of a monero transaction can be seen below.

Graphical user interface, application

Description automatically generated

Furthermore, Monero forces you 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 linkage property is also what prevents double spending on a blockchain. Meaning you can mathematically use a UTXO only once in monero, while in bitcoin you must believe that miners have validated the block properly. This increases privacy at the cost of computation and the use of

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.

The downside of monero is that ring signatures require more computation power and the even bigger downside is that the required storage space for each transaction is much larger. As of 2022 the average monero transaction takes up 1420 Bytes[[8]](#footnote-8), while the average Bitcoin transaction takes up 224 Bytes[[9]](#footnote-9)

* + - 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 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 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. Legal Ramifications
2. Conclusion

Although privacy seems to be weaker in bitcoin it all depends on how the user acts. In bitcoin a user can sign things with their private keys to prove all their transactions will be known. In Monero a user can make a transaction where they try to double spend and since that is impossible it proves which transactions belong to said user. In z-cash a user can …

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. The deanonymization happens elsewhere and so the legal ramifications should happen there as well?

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

1. Art. 4 GDPR, Definition: https://gdpr-info.eu/art-4-gdpr/ [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. https://www.ibm.com/docs/en/zos/2.1.0?topic=keys-rsa-private-public [↑](#footnote-ref-3)
4. https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/ [↑](#footnote-ref-4)
5. Art. 17 GDPR [↑](#footnote-ref-5)
6. [↑](#footnote-ref-6)
7. https://eprint.iacr.org/2020/018 [↑](#footnote-ref-7)
8. https://xmrchain.net/ [↑](#footnote-ref-8)
9. https://bitcoinfees.earn.com/#fees [↑](#footnote-ref-9)