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)

{Beachten Sie bitte allfällige abweichende Anforderungen der einzelnen Institute oder Departemente. Die hier verwendete Schriftart ist Univers, teilweise wird Arial oder Times verlangt}

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)

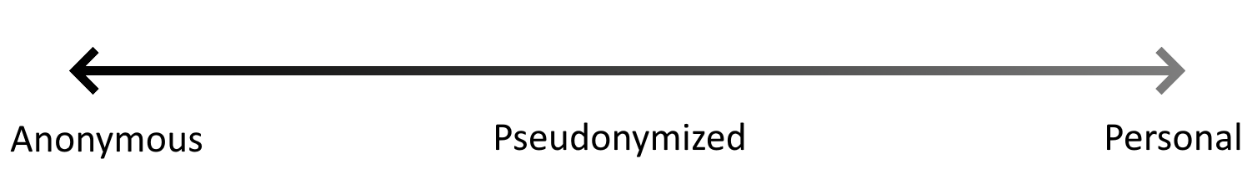
1. Introduction
   1. Personal, anonymous and pseudonymized data

There are many types of data in our current world. Among these, the Information which concerns us the most is personal data. Personal data is data, which can be directly linked to a natural person through direct means. An example of this would be a person’s medical record or anything containing names, addresses, birthdays and so on.

After personal data there is pseudonymized data. This is information, that can be linked through indirect means to a natural person, such as knowing a person’s wallet address. If data cannot be linked to a person through any means it is anonymous data and is outside of most laws.

This scale is continuous, and data can find itself anywhere in between the three data types.[[1]](#footnote-1)

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, and it refers to

UTXO based cryptocurrencies do not use wallets at a protocol level, as a user you must keep track of all your utxos to be in control of your assets.

1. Privacy in Distributed Ledgers
   1. UTXO vs Account Based Blockchains
   2. Different Cryptocurrencies

While banks protect privacy by releasing as little information as possible to the public, distributed public ledgers do not have that luxury. As the name implies, they must be accessible to everyone, and no information can be hidden. This makes privacy only possible through the means of cryptographic methods. Some notable ones include the usage 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 as a distributed online ledger. Already in 2008 privacy was a big concern.

Bitcoin is not fully anonymous, since if you can link a private key to a person. If a transaction had multiple UTXO inputs, then you can link these and their history to a person.

The main privacy problem appears when you have multiple inputs for a payment. Then you can link other transactions to the person.

The safety of a user also depends on the user themselves such as in banks. If someone leaks their own public key and always use the same key, then all their transactions become non private.

Diagram

Description automatically generated[[2]](#footnote-2)

* + 1. Privacy Coins
       1. Monero
       2. Dash

Dash uses a technique known as zero knowledge proofs to

* + 1. Metamask

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

1. Art. 4 GDPR, Definition: https://gdpr-info.eu/art-4-gdpr/ [↑](#footnote-ref-1)
2. Bitcoin: A Peer-to-Peer Electronic Cash System, Chapter 10: Privacy [↑](#footnote-ref-2)