Seminar Civil Law and Computer Science
Distributed Trust in Finance

Prof. Dr. Christian Cachin
Institute of Computer Science

Prof. Dr. Mirjam Eggen
Dr. Christian Sillaber
Institute for Civil Law

UNIVERSITÄT BERN

Topic description

How can privacy considerations be consolidated with transaction transparency?

Blockchain, as a decentralized and distributed public ledger technology in peer-to-peer network, applies a linked block structure to verify and store data, and applies the trusted consensus mechanism to synchronize changes in data, which makes it possible to create a tamper-proof digital platform for storing and sharing data. The model of many prominent blockchains consists of a pseudonymous transaction graph, visible on a public ledger. The senders and receivers of transactions are only represented by pseudonymous cryptographic keys. More recent blockchain networks also hide the transaction flow. Many blockchain variants are at odds with privacy requirements mandated by law. This currently hinders the adoption of blockchain technology. Trivial examples are the “right to be forgotten”, which is at odds with the design goal of tamper-proofness, as well as the requirement of “restriction of processing”, which is at odds with the requirement of most ledgers to store a full list of transactions forever.

1. Computer Science Task

Characterize the privacy levels of different cryptocurrencies:

- Describe how the payment structure works, what can be inferred about the history behind a “coin” in a transaction, and correlations visible between payments
- Optionally, describe how privacy can be attacked at the network level
- Include at least Bitcoin, Monero, and Zcash in your characterization, they provide a wide spectrum of different privacy levels

2. Law Task

Both the GDPR as well as the revDSG introduce several requirements which are at odds with public, permissionless blockchains. Using z.cash[1] as an example, answer the following questions:

- What justification(s) [Rechtfertigungsgründe] are the basis for data processing activities of different stakeholders in the project?

[1] See under: <https://z.cash/>.

- Which issues have been identified with regards to the GDPR and its application to public, permissionless blockchains? Please refer to the works published by the European Parliament.[2]
- Which issues are to be anticipated with regards to the revDSG and existing public, permissionless blockchains?

Materials/Literature

AKCORA CUNEYT GURCAN/GEL YULIA R./KANTARCIOGLU MURAT, Blockchain Networks: Data Structures of Bitcoin, Monero, Zcash, Ethereum, Ripple and Iota, in: CoRR abs/2103.08712, 2021, available under: <https://arxiv.org/abs/2103.08712>.

BAUMANN JONAS/HAMM NIKOLAS, Die Zuweisung datenschutzrechtlicher Verantwortlichkeit in private Blockchains, in: InTeR 2021, p. 208-212, available under: <https://www.swisslex.ch/de/doc/essay/26f4b24f-4a02-4872-a74c-3b2ddc75b953>.

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/EPRS_STU(2019)634445(ANN1)_EN.pdf>.

HERSKIND LASSE/KATSIKOULI PANAGIOTA/DRAGONI NICOLA, Privacy and Cryptocurrencies – A Systematic Literature Review. IEEE Access Vol. 8, 2020, p. 54044-54059, available under: <https://doi.org/10.1109/ACCESS.2020.2980950>.

ISLER MICHAEL, Datenschutz auf der Blockchain, in: Jusletter 4 Dezember 2017, available under: <https://jusletter.weblaw.ch/juslissues/2017/917/datenschutz-auf-der-_fbecc2b55b.html__ONCE>.

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-4894-92a1-30d3a353d37e/>.

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-3a44-4a60-8b27-6560ee7c4ef6>.

[2] Available under: <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019) 634445_EN.pdf>.