Seminar Distributed Trust in Finance
Prof. Dr. Christian Cachin
Prof. Dr. Mirjam Eggen
Dr. Christian Sillaber
Speaker: Marius Asadauskas, Lynn Grau

UNIVERSITÄT BERN

13.05.2022

How can privacy considerations be consolidated with transactions transparency?

Technical Aspects

Zero-Knowledge Proof criteria:

- **Completeness:** The proof must convince the verifier that you hold the secret
- **Zero-Knowledge:** The secret must not be revealed through the proof
- **Soundness:** The proof should be infeasible without knowledge of the secret

Z-Cash Mining reward distribution:

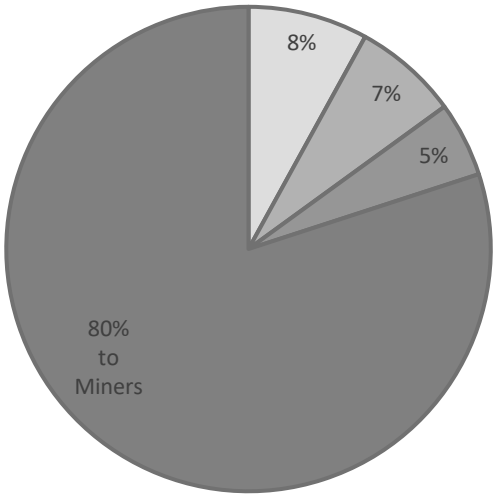

Figure 1: <https://z.cash/zcash-development-and-governance/> (last recalled 8.5.22)

Legal Aspects

Many blockchains are at odds with the legal requirements of data protection acts. Public permissionless blockchains are more problematic because of their lack of control over which actors have access to the relevant data. However, a case-by-case analysis needs to be assessed to determine the exact problems.

The General Data Protection Regulation (GDPR) applies wherever personal data is processed, article 4(1) GDPR determines what data qualifies to be personal:

*'**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

Data which is normally processed on public permissionless blockchains are: public keys, transactional data, extended content data and data saved "off-chain". Other categories of data that aren't public keys but may be used on blockchains are transactional data, such as names or addresses.[1] This kind of data can with appropriate technical utilities be used to identify a person, therefore they aren't anonymous but pseudonymous and qualify to be personal data under the GDPR. Public permissionless blockchains rely on several formally independent participants to maintain and run the system.[2]

Since the justification for personal data processing must be done by the data controller, it also needs to be determined which stakeholders qualify to be data controller. The identification of a data controller is very important because it is the entity which is responsible to comply with the obligations under the GDPR and need to enforce the rights of the data subjects. It is difficult to determine a data controller in blockchains since they are by their nature decentralized and designed to be operated by many parties.[3] However, the decentralization is put into question in the cryptocurrency Zcash, since founders hold more than 10% of all the z-cash coins.[4] It is therefore to be considered if the founders of Zcash qualify to be a legal entity and could be seen as data controller under the GDPR.

Every stakeholder might have different interests regarding the system, this results in different focuses in the design of blockchains. Zcash set their focus on privacy and provides higher anonymity and privacy than other cryptocurrencies. With the use of zk-SNARKS Zcash has the potential to facilitate the right for 'data protection by design' because users can decide if they want the other party to see their transactional data.[5] However only a small amount of transaction is made with z-addresses, the majority are t-transactions where transactional data is also public on the blockchain.[6]

The revised Data Protection Act is very similar to the GDPR[7] and similar problems are to be anticipated when it will come into force. Both are designed that the data which can be processed can be modified and deleted, especially to enforce the data subject rights. To ensure the trust and data integrity in blockchains data is permanent and can hardly be deleted or modified.[8] The enforcement of the data subject rights is therefore problematic. Even though they are less extensive in the revDPA than they are in the GDPR, tensions will arise. However, the exact impact of the revDPA can only be determined when it has been implemented in the Swiss jurisdiction.

---

[1] 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/EP RS_STU(2019)634445_EN.pdf> p.15.

[2] SCHMID ROMAN/ZIOLKOWSKI RAFAEL/ SCHWABE GERHARD: Together or Not? Exploring Stakeholder in Public and Permissionless Blockchains, Zurich Open Repository and Archive, p. 6098., 2022, available under: <https://www.zora.uzh.ch/id/eprint/211821/1/0595-2.pdf>.

[3] EPRS study, p. 42.

[4] Coindesk, "Zcash," [Online]. Available: <https://www.coindesk.com/learn/crypto/zcash/.> (Last recalled on 3.5.22).

[5] European Parliament (27 November 2018) Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018) para 21.

[6] The Basics: < https://z.cash/the-basics/>. (last recalled 7.5.22)

[7] BAERISWYL BRUNO: Der «grosse Bruder» DSGVO und das revDSG: Ein vergleichender Überblick, SZW 2021, p. 9.

[8] EPRS Study, p. I.