Is GDPR a Roadblock to Blockchain?

1. Swiss Symposium Blockchain Research, Zurich, May 14th
Jörn Erbguth, Dipl.-Inf., Dipl.-Jur.
Consultant Legal Tech, Blockchain, Smart Contracts and Data Protection
PhD candidate, University of Geneva

joern@erbguth.ch +41 787256027

Agenda

- Article 8 of the Charter of Fundamental Rights and GDPR

- The main conflicts of blockchain & GDPR

- How to evaluate GDPR compliance

- 5 ways that blockchain applications can cope with GDPR

Charter of Fundamental Rights of the European Union

Article 8

Protection of personal data

1.   Everyone has the right to the protection of personal data concerning him or her.

2.   Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3.   Compliance with these rules shall be subject to control by an independent authority.

What does the GDPR protect?

Art. 1 GDPR
Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

GDPR in Relation to Other Fundamental Rights

Recital 4

Data protection in balance with other fundamental rights*

[1] The processing of personal data should be designed to serve mankind. [2] The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. [3] This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.
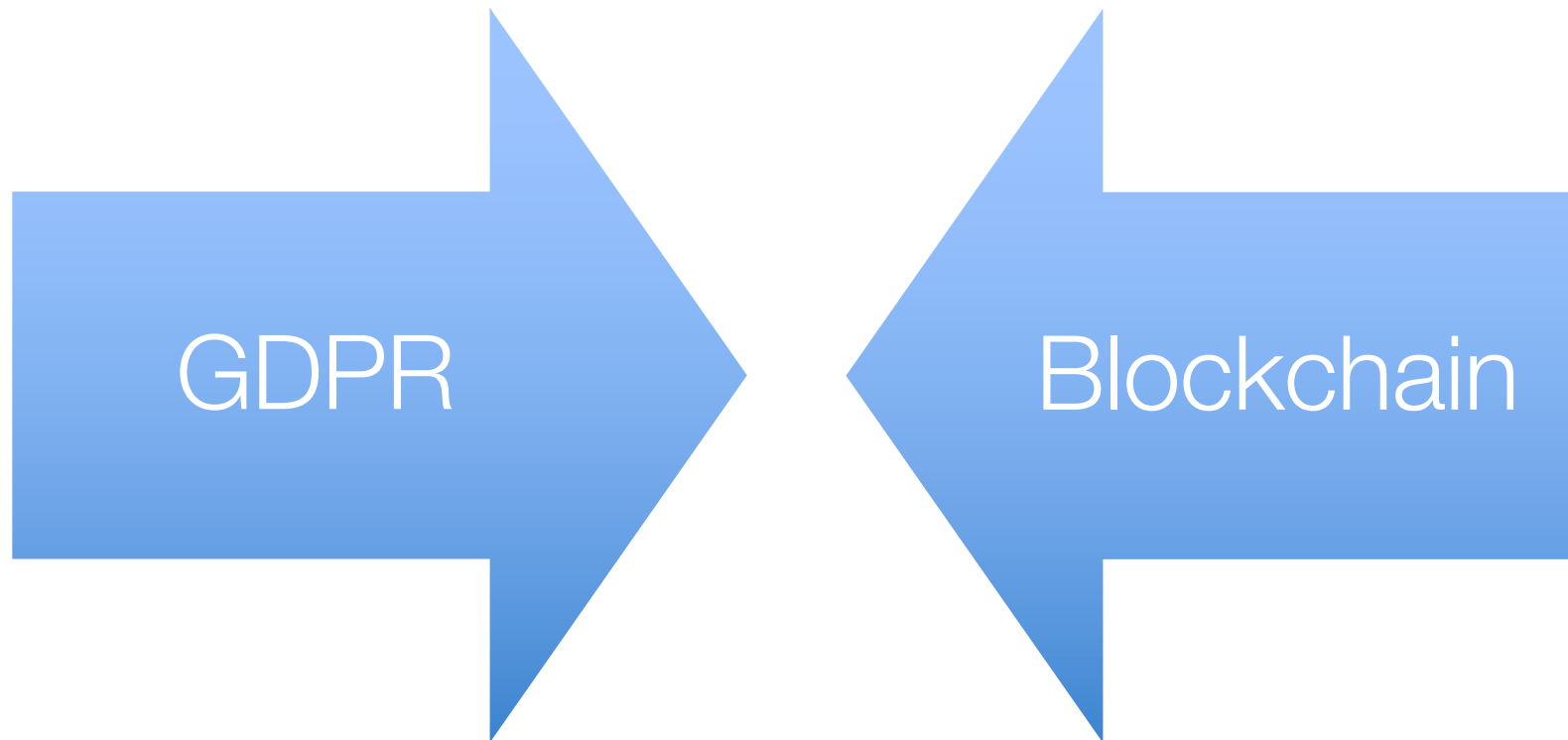
GDPR vs. Blockchain
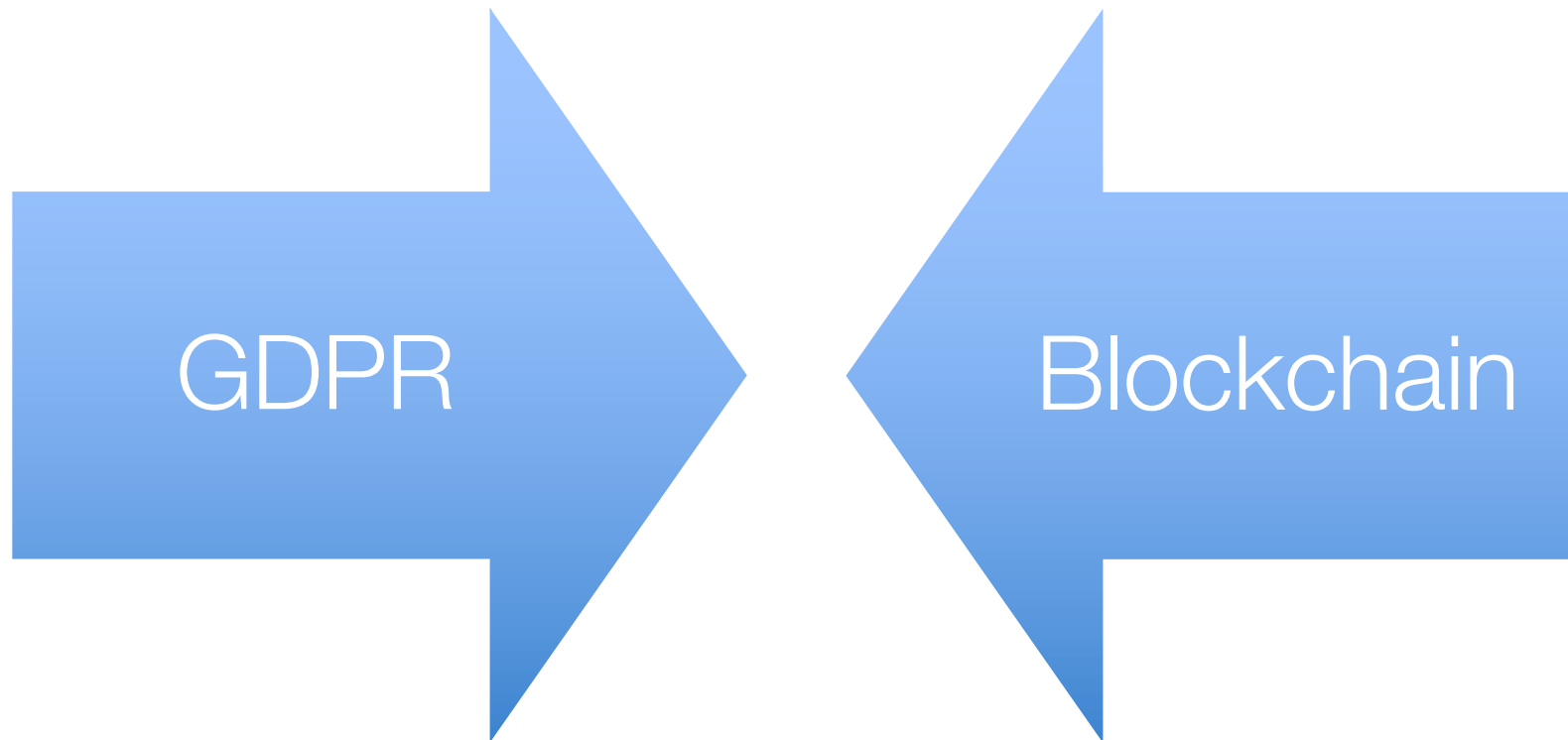
Right to …

Art. 16: rectification   immutable

Art. 17: erasure   public

Art. 18: restriction of processing

GDPR vs. Blockchain

GDPR → ← Blockchain

Clear responsibilities
controller
processor

distributed responsibility
anonymous participation

General Data Protection Regulation (GDPR)

- Processing of personal data is forbidden

- Unless there is proper justification

- Obligations for controllers and processors

- Rights for data subjects

- Includes obligation to information security

- Fines up to 20 mill. € or 4% of worldwide annual turnover

How to evaluate GDPR compliance

- Does GDPR apply?

- Is there processing of personal data?

- Is there a justification for the data processing?

- Do I comply with the obligations of GDPR?

Does the GDPR apply? (Art. 2, 3)

- Some entity that is considered a controller or a processor is in the EU

- Offering goods or services to data subjects in the EU

- Monitoring behavior of data subjects in the EU

- Not if only for personal use or household activity

Personal data (Art. 4.1)?

Any information relating to an identified or identifiable natural person

- Pseudonymous data is personal data

- Anonymous data is **not** personal data

Recital 26: To determine whether a natural person is identifiable, account should be taken of **all the means reasonably likely to be used** ... either by the controller or by another person to identify the natural person directly or indirectly.

Examples of personal data

- ✓ IP addresses

- ✓ Bitcoin addresses

- ✓ "anonymized" movement profile

- ✓ "anonymized" browsing history

- ✗ aggregated movement profiles

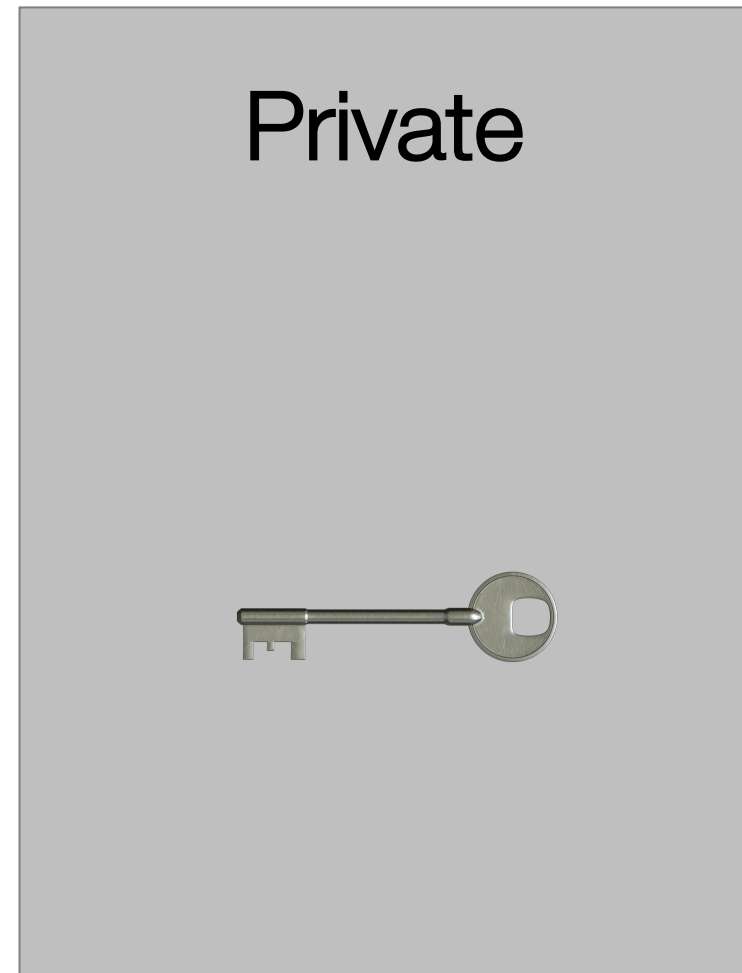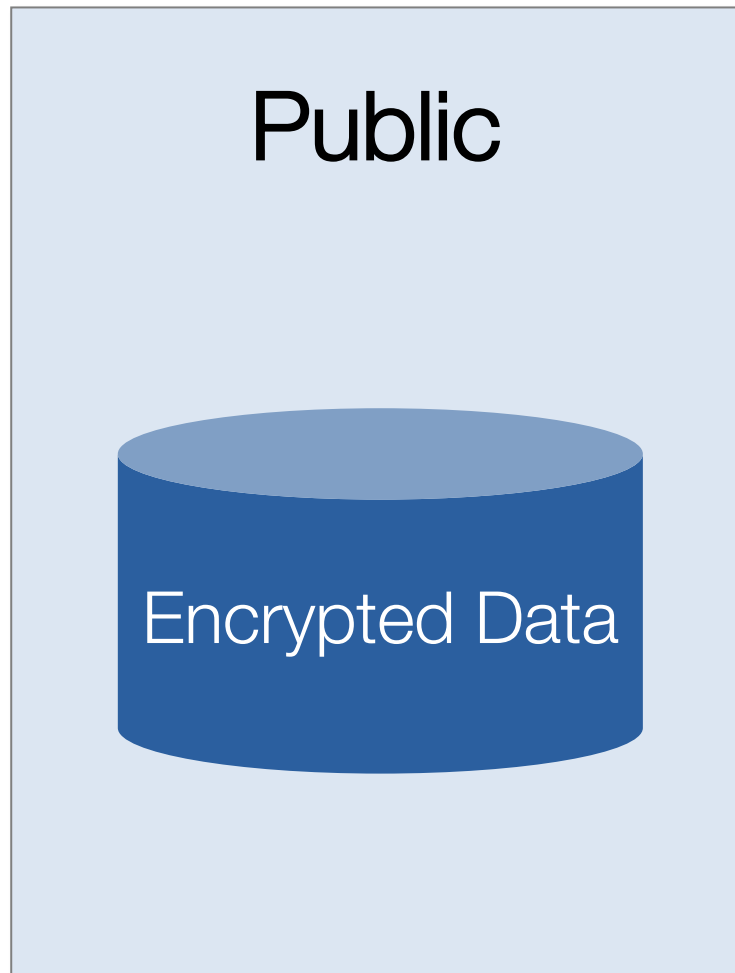- ✗ aggregated browsing history

Attention: Look at the individual case – do not generalize

Encryption

Deletion of the encryption key = deletion of the content?

Use of Hash Values

Public

Encrypted Data

Private

Use of Hash Values

Public

Private

Data
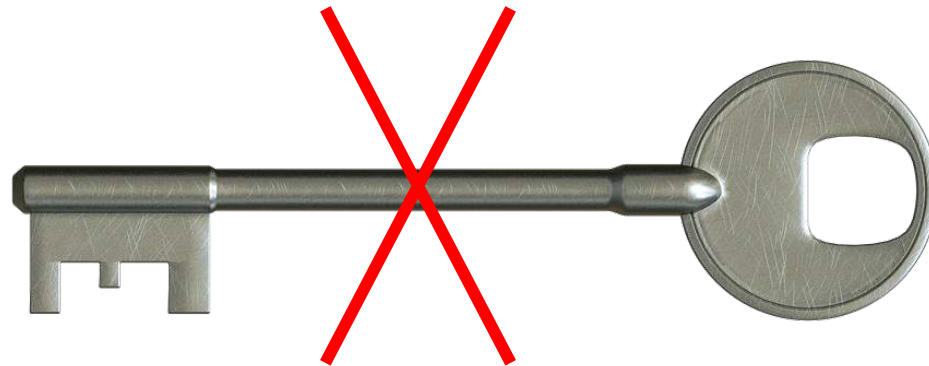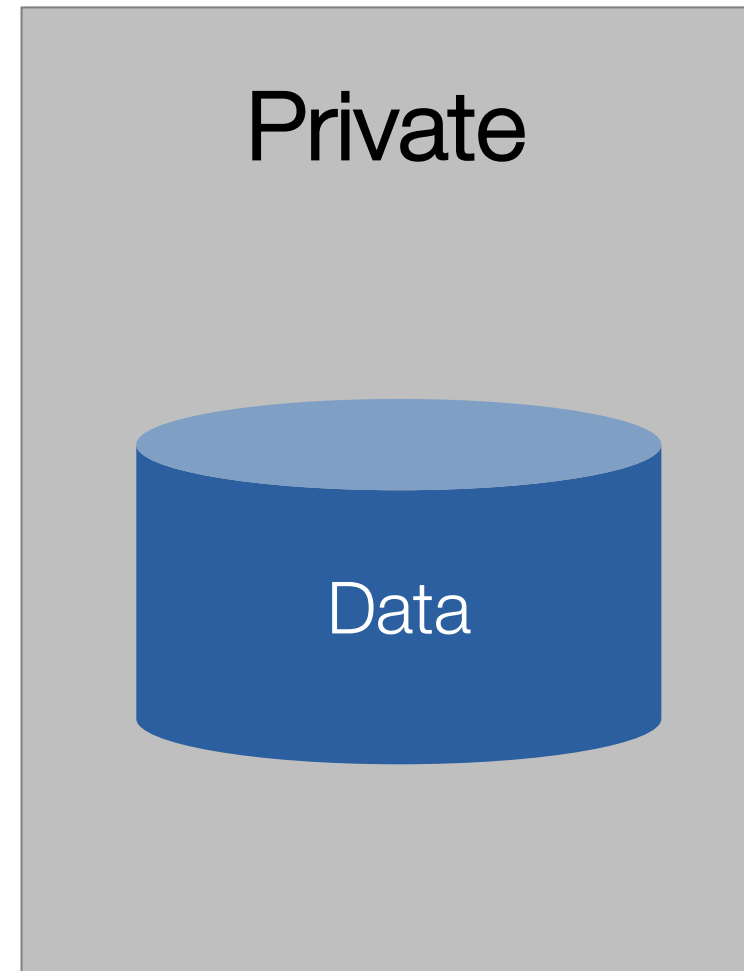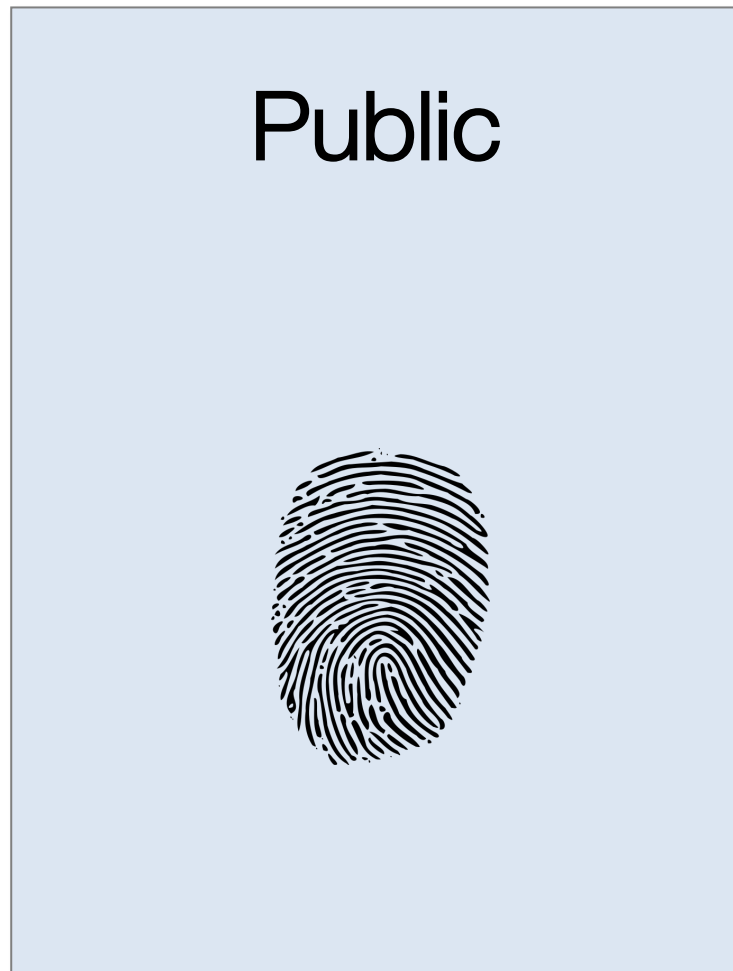
Cryptographic hash functions

- Serve as digital fingerprints

- Virtually unique

- Fixed length (e.g. 32 bytes)

- For digital objects of any size

ONE WAY

GDPR-compliant use of hash values

Non-GDPR-compliant use of hash values

has diploma

Adding Salt and Pepper to Hashes

- Ensuring enough **entropy**

- Making guessing practically impossible

- Can prevent rainbow table attacks

- Can prevent parallel attacks

How to Hash Data

Data

First Name	Last Name	Article	Quantity	Price
John	Smith	1984 by George Orwell	1	10
Lisa	Doe	Ulysses by James Joyce	1	20
John	Smith	Inside Wikileaks by Domscheit-Berg	1	15

Wrong solution

Off-chain

First Name	Last Name	Salt		Hash
John	Smith	8768374677692345 2362	→	8762764826745926 5308697
Lisa	Doe	9879360348574363 6365	→	9879698357934856 9273643

On-chain

Hash	Article	Quantity	Price
8762764826745926 5308697	1984 by George Orwell	1	10
9879698357934856 9273643	Ulysses by James Joyce	1	20
8762764826745926 5308697	Inside Wikileaks by Domscheit-Berg	1	15

How to Hash Data

Data

First Name	Last Name	Article	Quantity	Price
John	Smith	1984 by George Orwell	1	10
Lisa	Doe	Ulysses by James Joyce	1	20

Still problematic solution

Off-chain

First Name	Last Name	Article	Quantity	Salt		Hash
John	Smith	1984 by George Orwell	1	87683746776923452362	→	76482654672653086974532
Lisa	Doe	Ulysses by James Joyce	1	98793603485743636365	→	35793485692736433524132
John	Smith	Inside Wikileaks by Domscheit-Berg	1	29749850385739857395	→	86786876868594939653656

On-chain

Hash	Price
76482654672653086974532	10
35793485692736433524132	20
86786876868594939653656	15

How to Hash Data

Data

First Name	Last Name	Article	Quantity	Price
John	Smith	1984 by George Orwell	1	10
Lisa	Doe	Ulysses by James Joyce	1	20

Better solution

Off-chain

First Name	Last Name	Article	Quantity	Price	Salt		Hash
John	Smith	1984 by George Orwell	1	10	876837467762342362	→	1342587627648239265308697
Lisa	Doe	Ulysses by James Joyce	1	20	987936034854366365	→	1259879698357934856978757
John	Smith	Inside Wikileaks by Domscheit-Berg	1	15	29749850385739857395	→	8724619311098089768273687

On-chain

Hash
1342587627648239265308697
1259879698357934856978757
8724619311098089768273687
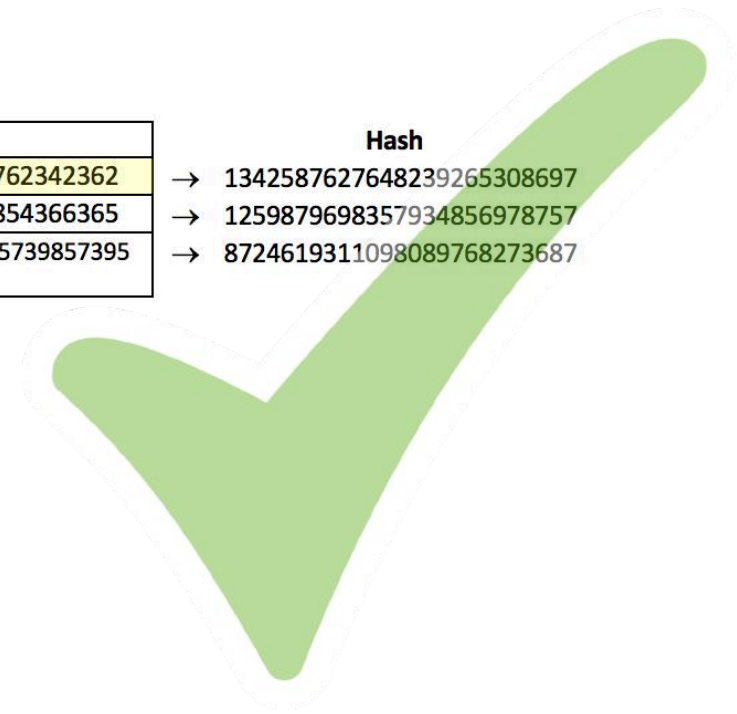
How to Hash Data

Data

First Name	Last Name	Article	Quantity	Price
John	Smith	1984 by George Orwell	1	10
Lisa	Doe	Ulysses by James Joyce	1	20

Also a better solution

Off-chain

First Name	Last Name	Article	Quantity	Price	Salt		Hash
John	Smith	1984 by George Orwell	1	10	876837467762342362	→	134258762764823926530 8697
Lisa	Doe	Ulysses by James Joyce	1	20	987936034854366365	→	125987969835793485697 8757
John	Smith	Inside Wikileaks by Domscheit-Berg	1	15	297498503857398573	→	980928743109323948235 7898

On-chain

Hash	Price
134258762764823926530 8697	10
125987969835793485697 8757	20
980928743109323948235 7898	15

Test: Can you derive Personal Information?

Is it possible to derive data from the blockchain even when all information outside the blockchain is deleted?

What if

- somebody knows one transaction, can she see further transactions of the same person?

- somebody knows part of a transaction, can she see further details?

- somebody knows personal details of a person, can she discover information about that person's activity?

Zero-Knowledge Proof

Proof of knowing something
without revealing it

Zero-Knowledge Proof – Zcash

- Limiting the purpose of using personal data by technical means

- Only the correctness of the transaction can be proven

- Privacy by design
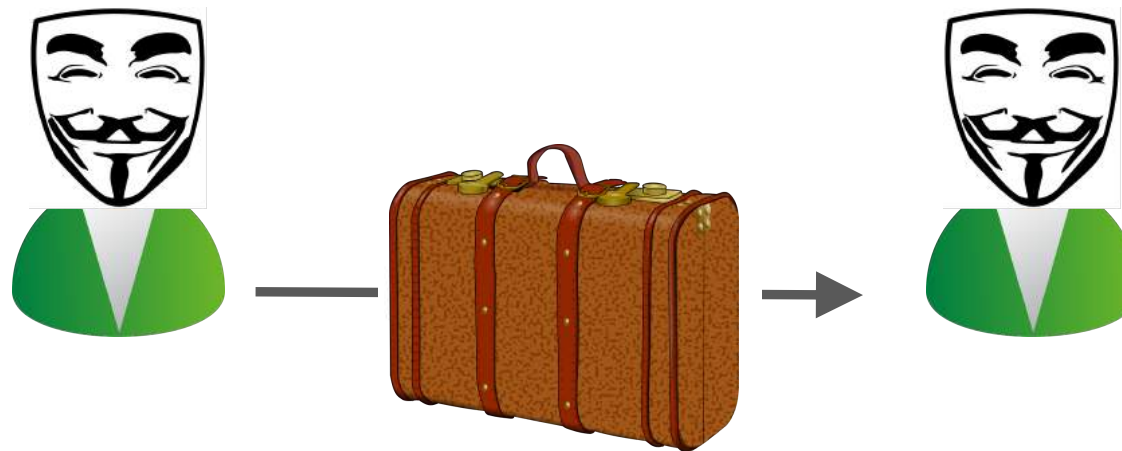
Advantages

- Protection also against insiders (e.g. admins)

- Access rights cannot be modified retroactively

- Protection against intruders that breach the firewall

- Data is protected against manipulation

Lawfulness of processing (Art. 6)

- Consent (Art. 6.1 a)

- Performance of a contract (Art. 6.1 b)

- Compliance with a legal obligation (Art. 6.1 c)

- Legitimate interest (Art. 6.1 f)

Controllers, Processors, Data Subjects

Controller — Determines the purposes and means of processing

Processor — Processes data on behalf of the controller

Data-Subjects

Who is "Controller" and who is "Processor"?

- Node operators?

- Miner who mines a specific block?

- All miners together?

- User who signs a transaction with her private key?

- Exchange or wallet service that signs a transaction on behalf of a user?

- Entity that administrates permissions for a permissioned blockchain?

Opinion of the CNIL on Controllers and Processors

- User of a public blockchain is a controller

- Somebody who creates and controls a permissioned blockchain is a controller

- Members of a consortium can be joint controllers

- Node operators are processors

- Smart contract developers can be processors, if they retain control

Duties of Controllers and Processors

- Controllers must identify themselves

- Controllers are responsible towards data subjects

- Controllers must have processing agreements with processors

- Controllers must control processors

- Processors must process data only on documented instructions from the controller

Five Ways to Cope with GDPR

- Do not put any personal data (at all) on a blockchain

- Use Privacy Enhancing Technology and ensure that no personal information can be derived from the blockchain

- Obtain a justification that is permanent

- Let users put the data on a public blockchain themselves

- Build specialized blockchains that forget

Blockchain

GDPR Quick Check
beta test V0.2

https://erbguth.ch/QuickCheck

Thank you – Questions?