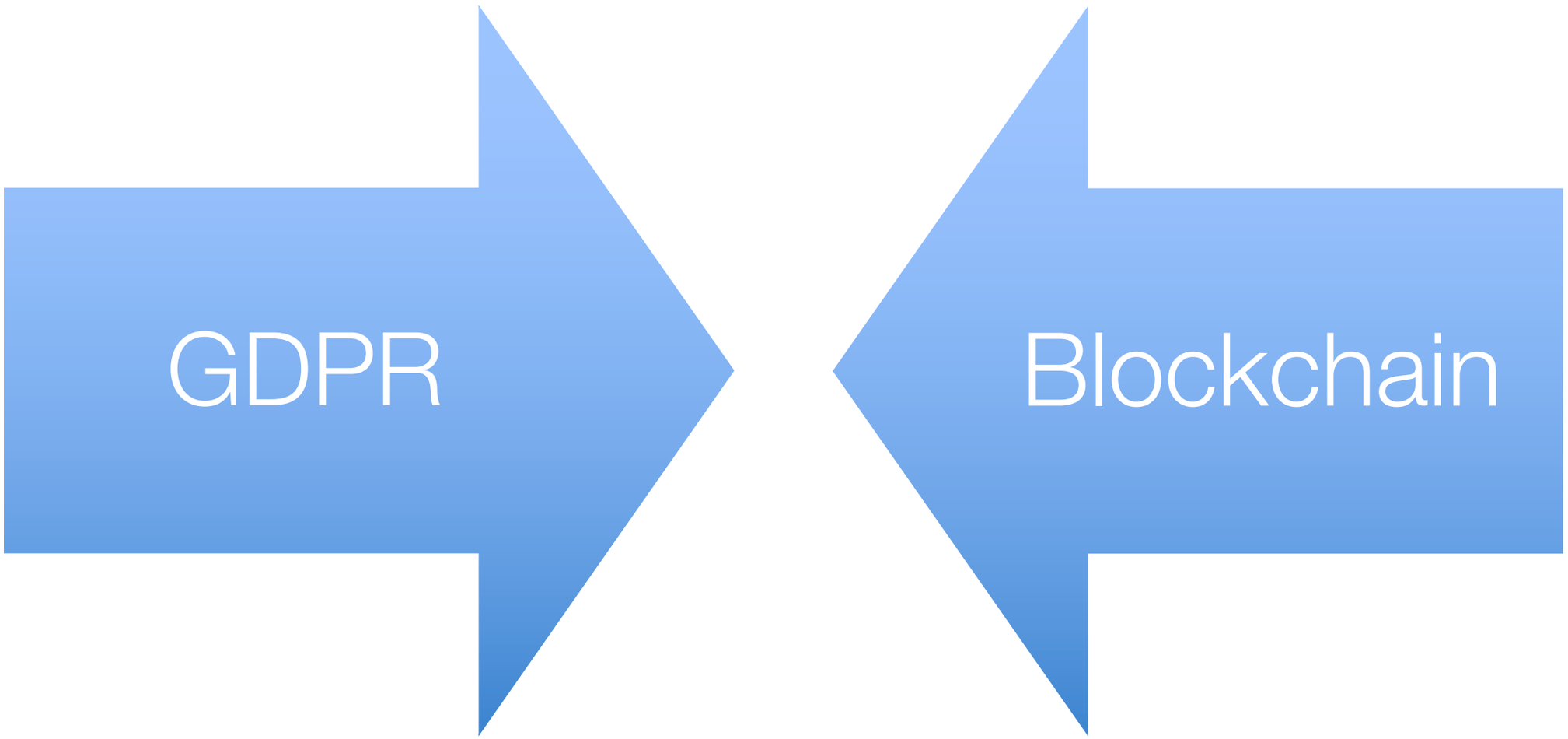
Blockchain and GDPR

Blockstack Decentralizing the World Tour, December 18, 2018, Prague

Jörn Erbguth, Dipl.-Inf., Dipl.-Jur.
Consultant Legal Tech, Blockchain, Smart Contracts and Data Protection

joern@erbguth.ch +41 787256027

GDPR vs. Blockchain



Right to …

Art. 16: rectification

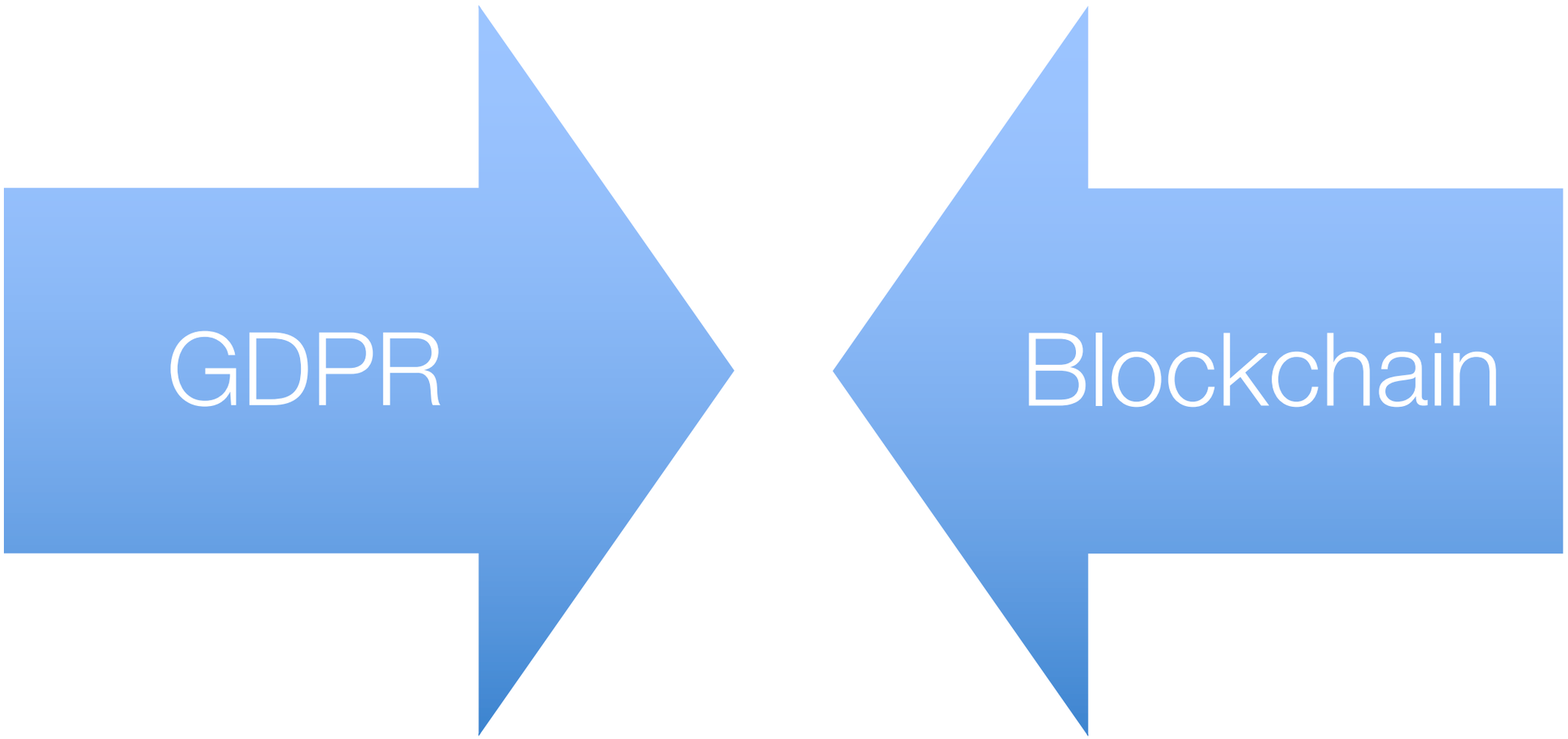
Art. 17: erasure

Art. 18: restriction of processing

immutable

public

GDPR vs. Blockchain



Clear responsibility
controller
processor

distributed responsibility
anonymous participation

General Data Protection Regulation (GDPR)

- Directly applicable European law
- Processing of personal data is forbidden
- Unless there is proper justification
- Obligations for controllers and processors
- Rights for data subjects
- Fines up to 20 mill. € or 4% of worldwide annual turnover

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.

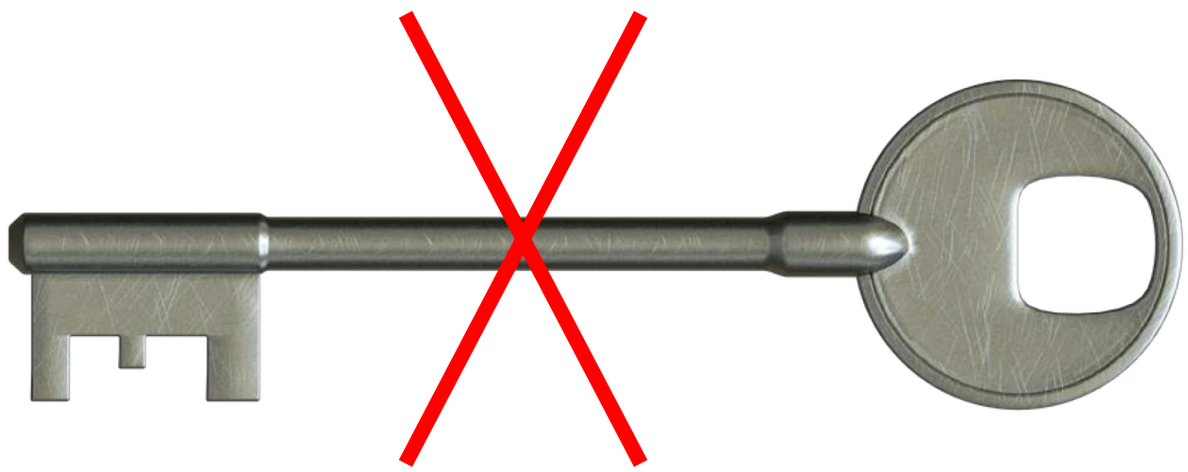
Examples of personal data

- ✓ 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

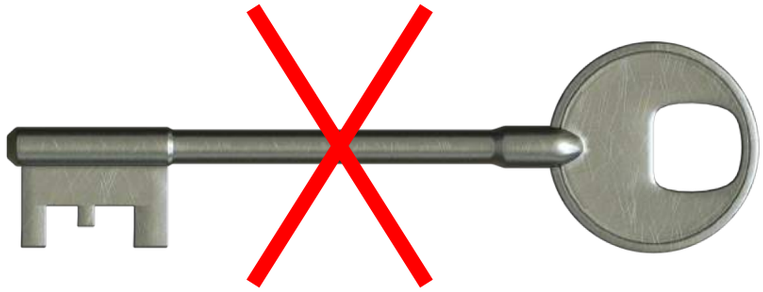
Deletion of the encryption key = deletion of the content?




SAMSUNG
MMCQE28GFMUP – MVA
DFK3OOA842 – SE842A0588
0842
REV 0
F/W VAM05S1Q
Model : Slim 128GB uSATA MLC
SSD P/N : MMCQE28GFMUP – MVA
WARRANTY VOID IF REMOVED
Solid State Drive RATED: DC+3.3V 0.32A SAMSUNG ELECTRONICS CO., LTD
WARNING DELICATE PRODUCT SENSITIVE PARTS INSIDE. DAMAGE MAY OCCUR IF SHOCKED. TOUCHING THE CIRCUITS MAY CAUSE MALFUNCTION. REMOVAL OF THIS COVER WILL VOID ANY AND ALL WARRANTIES.
Slim 128GB uSATA MLC
SEC – M – SLIM28GUSATA(B)
2008.10.07
SAMSUNG
MMCQE28GFMUP – MVA
SAMSUNG 837
K9HCG78U1M
PCK0

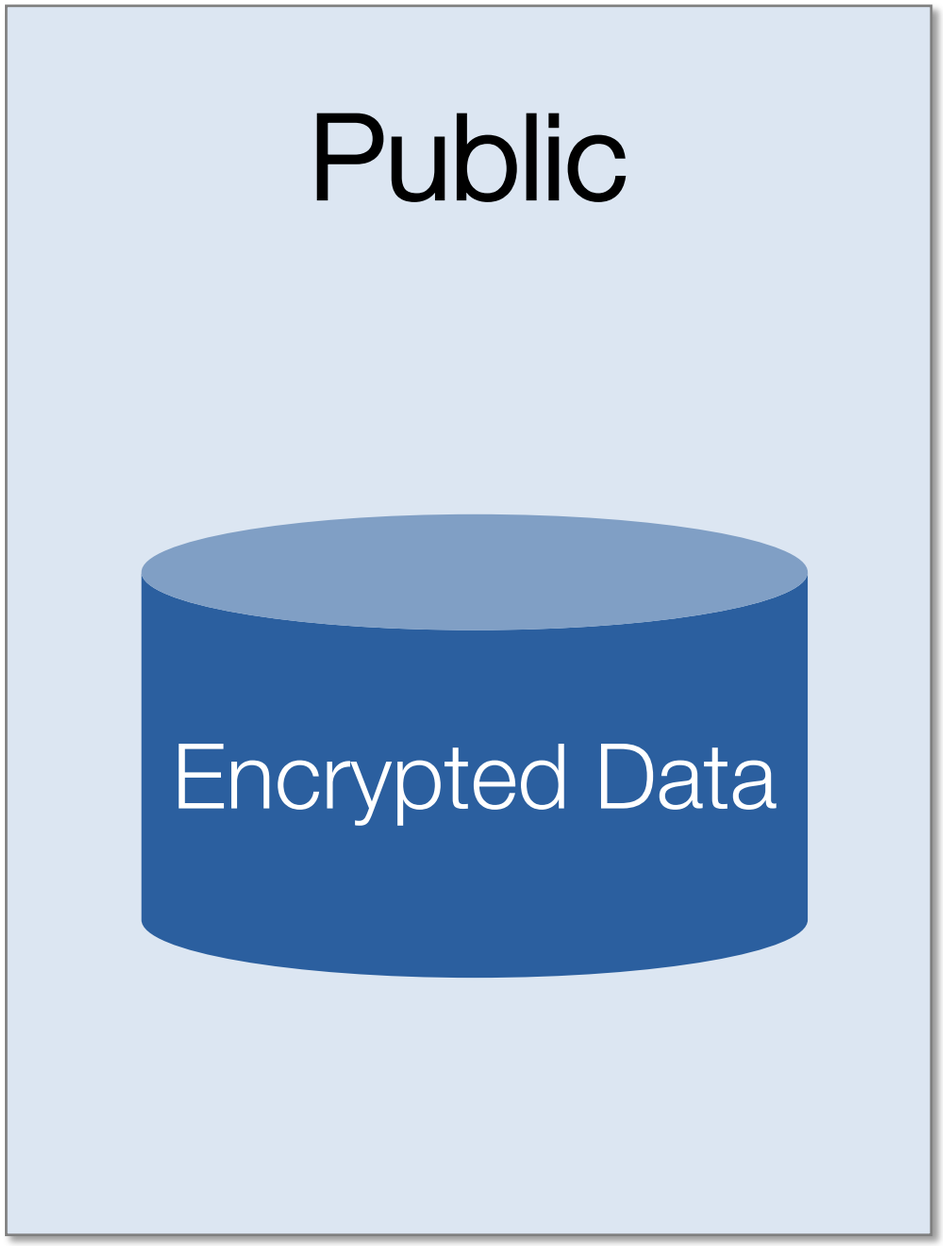
GDPR-compliant deletion?

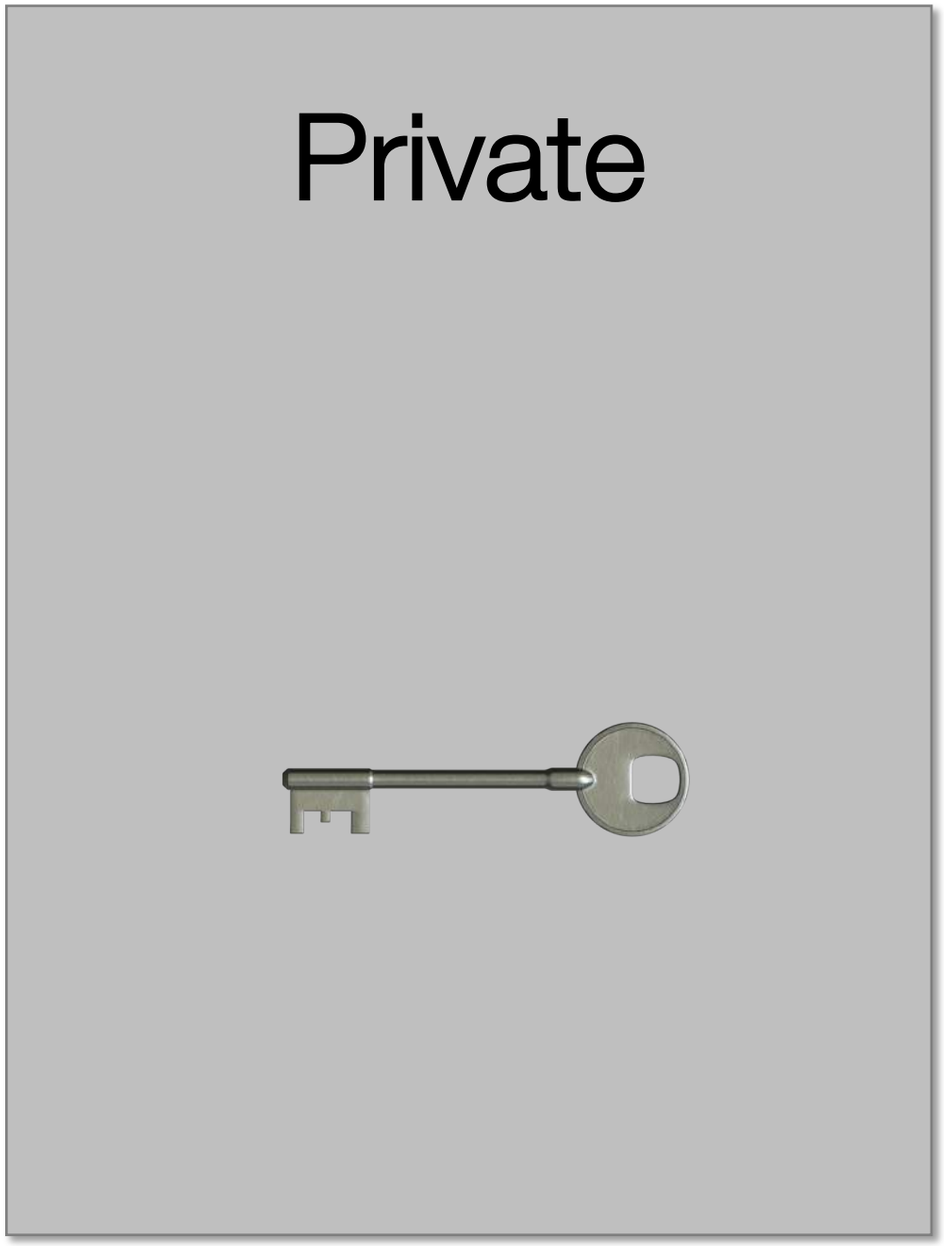
- Deletion of the encryption key = deletion of the content?



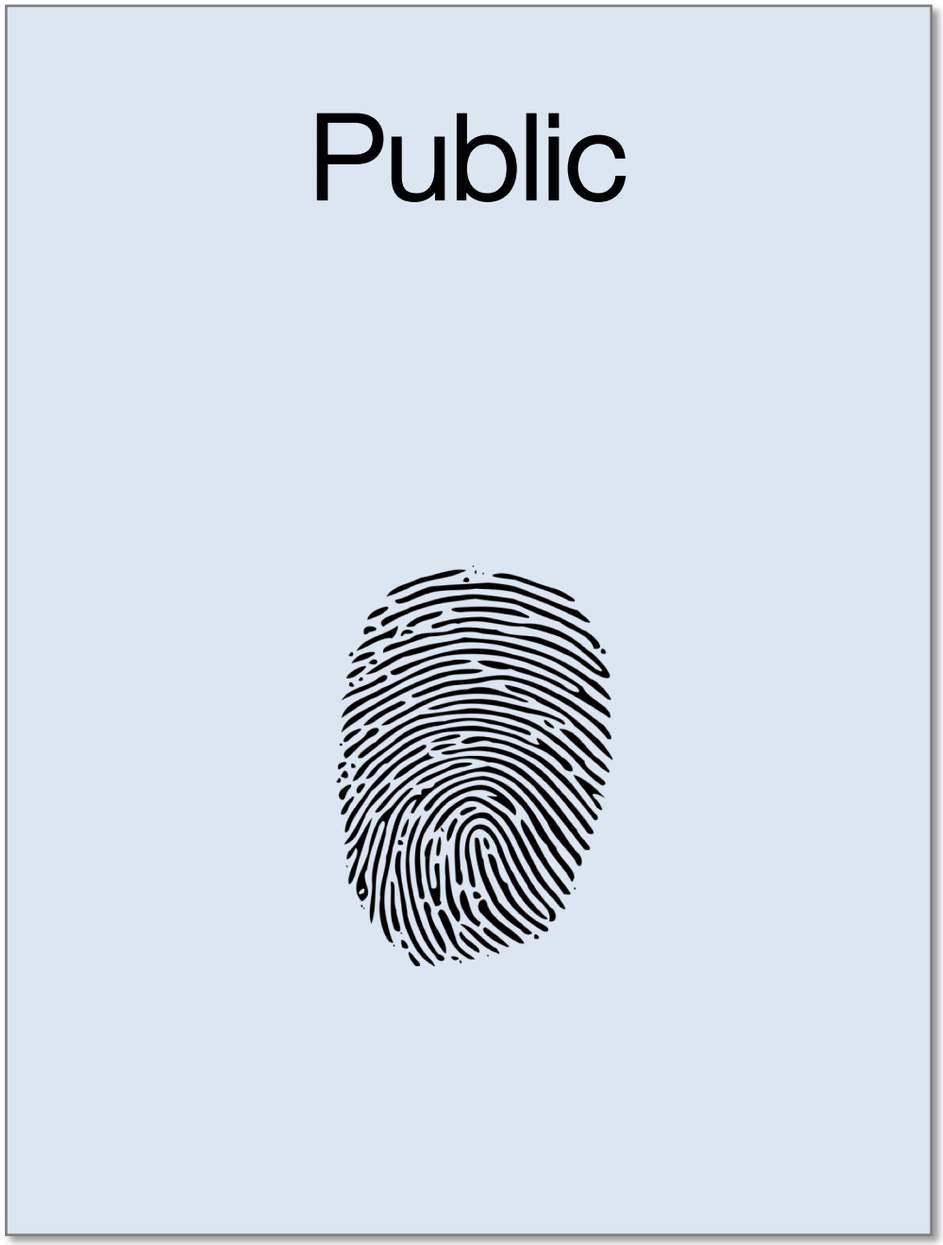
- Is there a remaining copy of the key?
- Will the encryption method become insecure in the future?

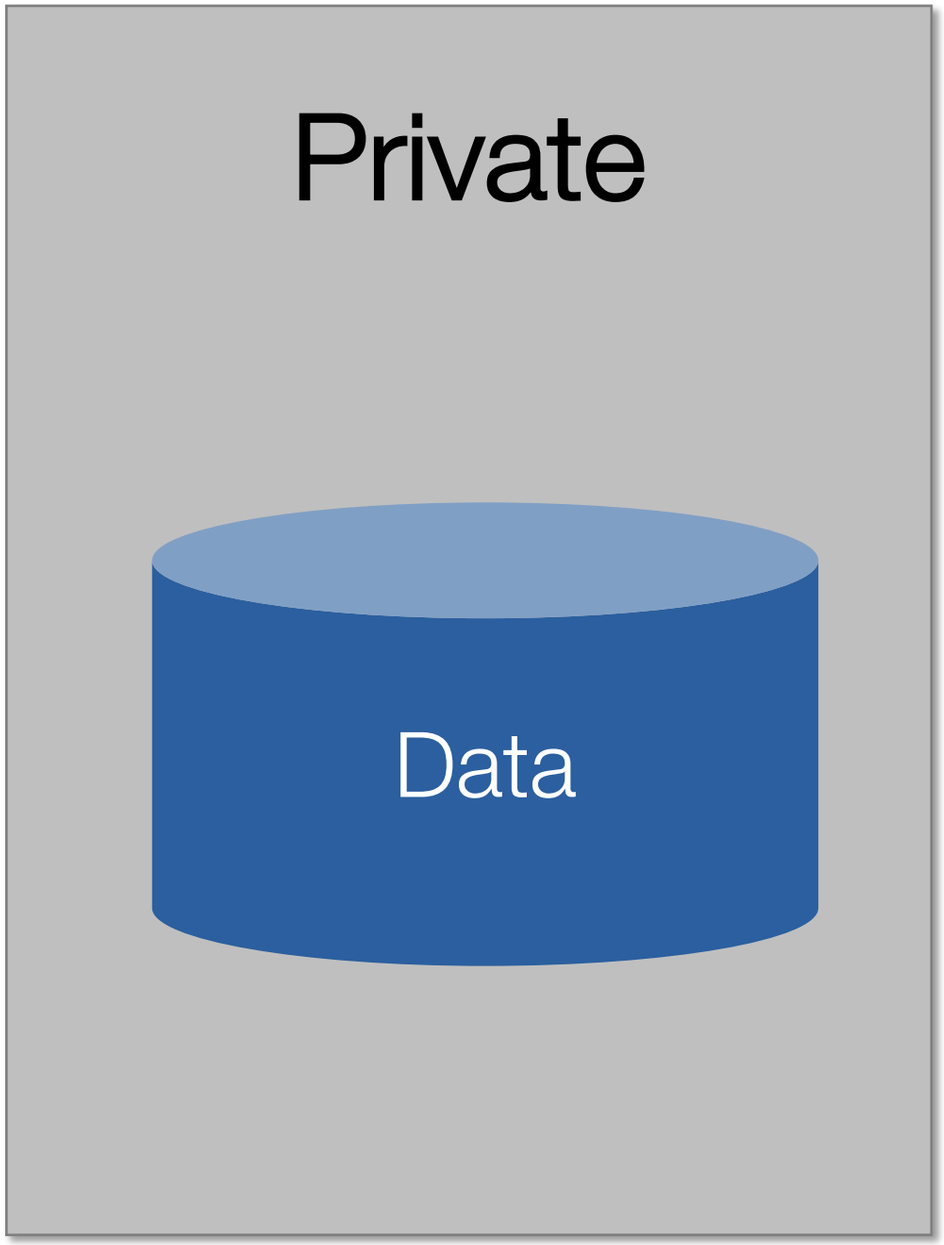
Use of Hash Values



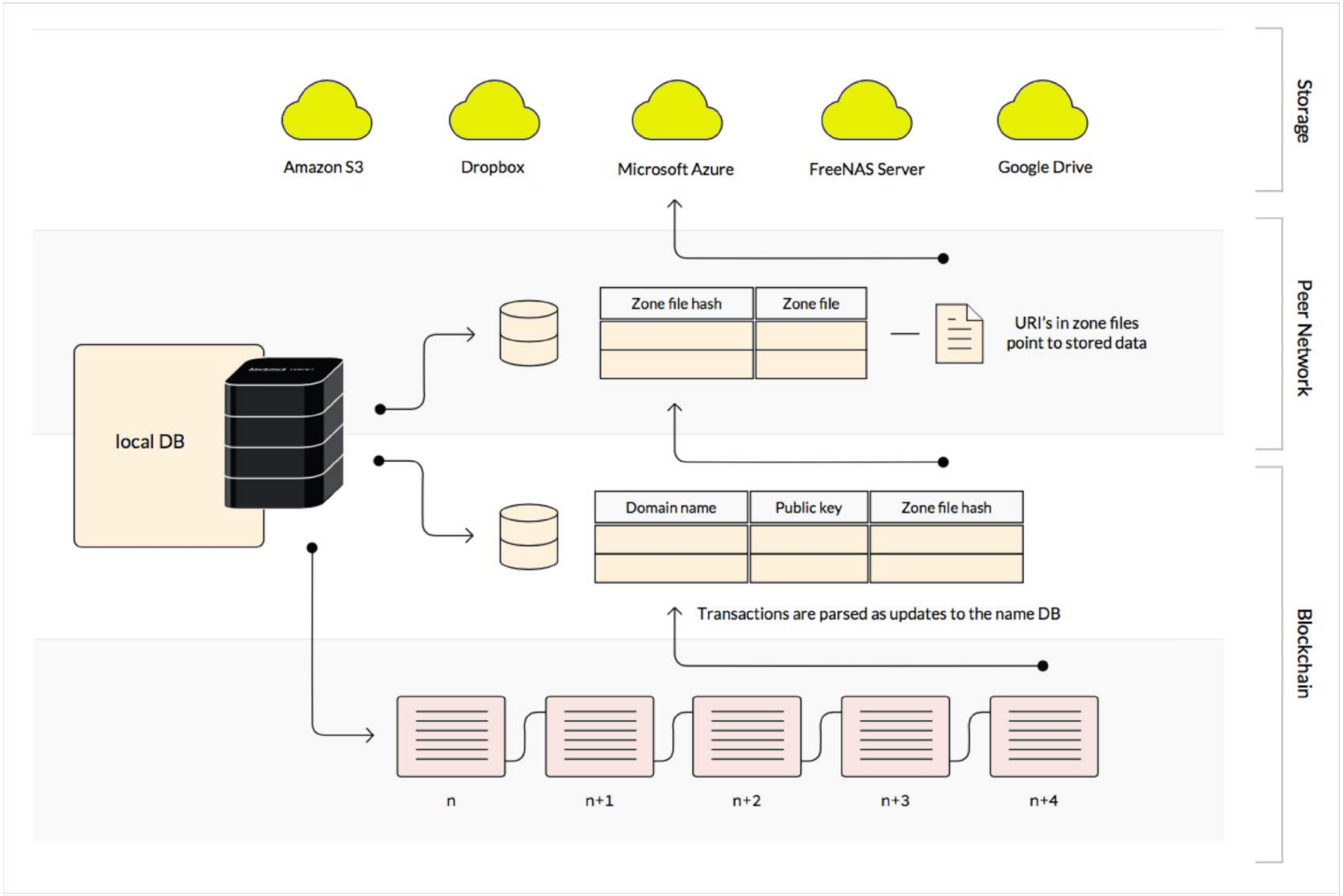


Use of Hash Values





Blockstack Architecture



Cryptographic hash functions

- Serve as digital fingerprints
- Virtually unique
- Fixed length (e.g. 32 bytes)
- For digital objects of any size
- One-way function

Demo 2

Examples of cryptographic hashes

- Switzerland `2275583196D791405892AACA0D87743C872F3FC0CF3308A6C3EF82528918AA8A`
- Switzerland. `43CF6F3ECA7253FFAB1FD5104172280189B91FDD5FA26774FCA6475FFA1E2EC9`
-  `8C4B4C4E211BA8C1A62DE2A3A6CA5AC8BFF501C14410100DD90D5077A0AC061E`

Kryptografische Hashwerte, datenschutzkonform

UNIVERSITÄT PASSAU

Universität Passau
Juristische Fakultät

Diplomurkunde

Die Juristische Fakultät der Universität Passau verleiht mit dieser Urkunde

Herrn **Jörn Horst Erbguth**

geboren am 5. Dezember 1967 in Marl

den akademischen Grad

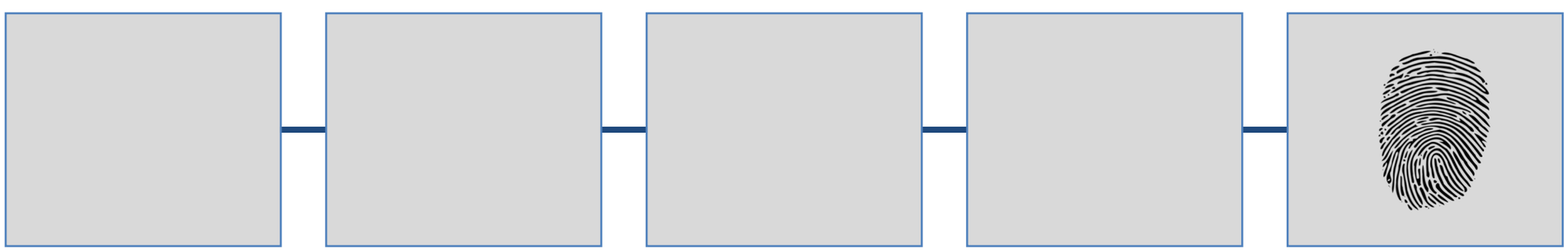
Diplom-Jurist Univ.

(Dipl.-Jur. Univ.)

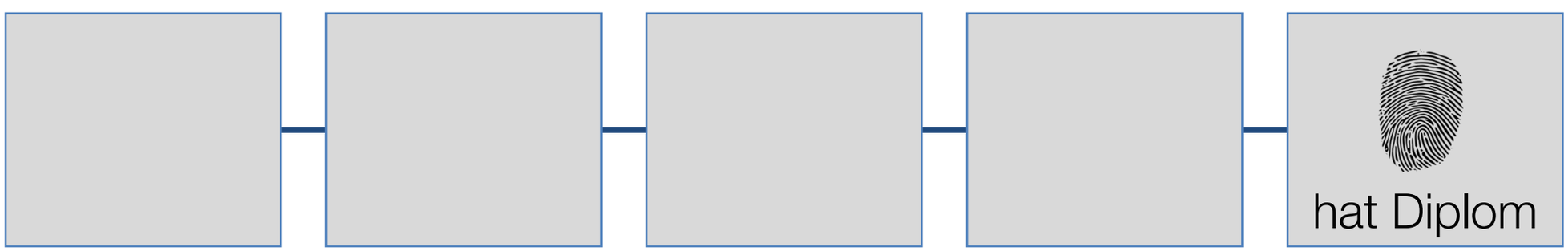
aufgrund der gemäß Ausbildungs- und Prüfungsordnung für Juristen (JAPO) in der jeweils gültigen Fassung am 23. Juli 1992 bestandenen Ersten Juristischen Prüfung.

Passau, den 24. Januar 2018

(Prof. Dr. Hans-Georg Dederer)
Dekan



Kryptografische Hashwerte, nicht datenschutzkonform



Use cases for cryptographic hash functions

- Validate external documents
- Time-stamping
- Proof of Existence
- Basic functionality for cryptography and DLT

The wrong use of hash functions can lead to the identification of data subjects!

Adding Salt and Pepper to Hashes

- Ensuring enough **entropy**
- Making guessing really hard
- 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	87683746776923452362	→	876276482674592653086 97
Lisa	Doe	98793603485743636365	→	98796983579348569273643

On-chain

Hash	Article	Quantity	Price
876276482674592653086 97	1984 by George Orwell	1	10
98796983579348569273643	Ulysses by James Joyce	1	20
876276482674592653086 97	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	→	7648265467265308697453 2
Lisa	Doe	Ulysses by James Joyce	1	98793603485743636365	→	3579348569273643352413 2
John	Smith	Inside Wikileaks by Domscheit-Berg	1	29749850385739857395	→	8678687686859493965365 6

On-chain

Hash	Price
764826546726530869745 32	10
357934856927364335241 32	20
867868768685949396536 56	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	→	134258762764823926530869 7
Lisa	Doe	Ulysses by James Joyce	1	20	987936034854366365	→	125987969835793485697875 7
John	Smith	Inside Wikileaks by Domscheit-Berg	1	15	297498503857398573	→	980928743109323948235789 8

On-chain

Hash	Price
1342587627648239265308697	10
1259879698357934856978757	20
9809287431093239482357898	15

Test: Does your system leak personal data?

Does the system disclose personal data by itself?

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 the person's activity?

Zero-Knowledge Proof

Proof of knowing something
without revealing it

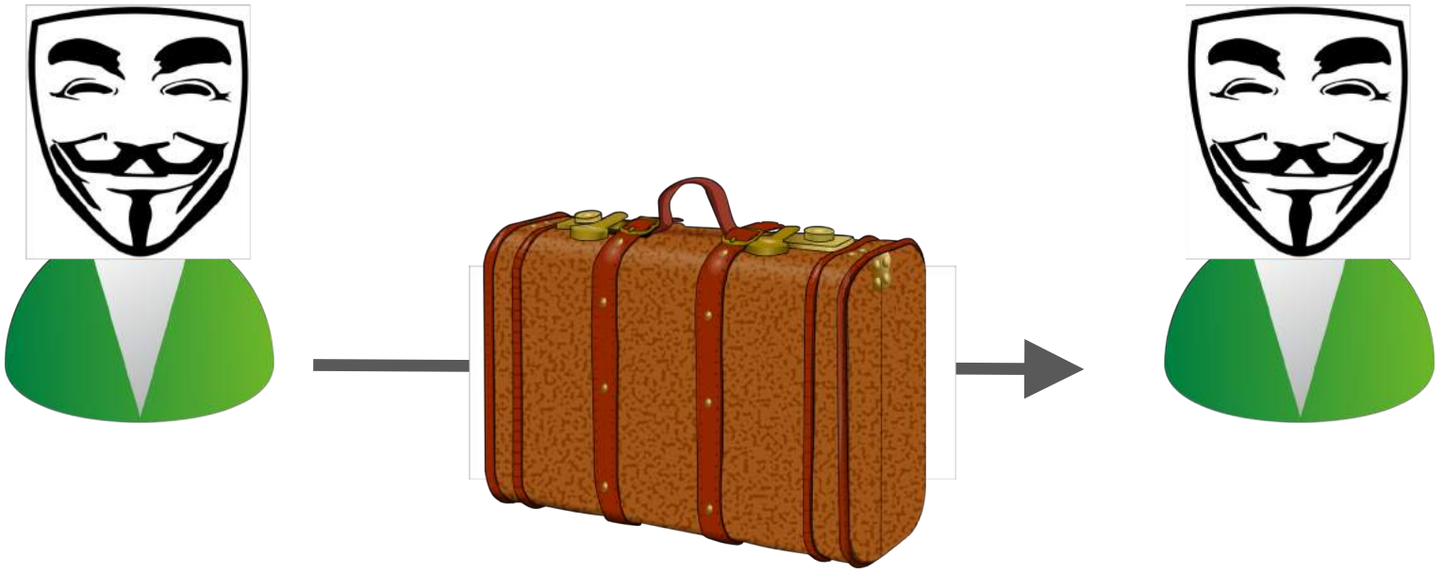
Simple Zero Knowledge Proof

Zero-Knowledge Proof – example

color vision

Zero-Knowledge Proof – Zcash

- Technical purpose limitation of personal data
- Only the correctness of the transaction can be proven



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

Still personal data?

- In a pre-GDPR opinion, DPAs said yes (Art. 29 WP, 05/14)
- GDPR says, it depends
- Risk that immutable data on blockchains become personal data later

Opinion of the CNIL

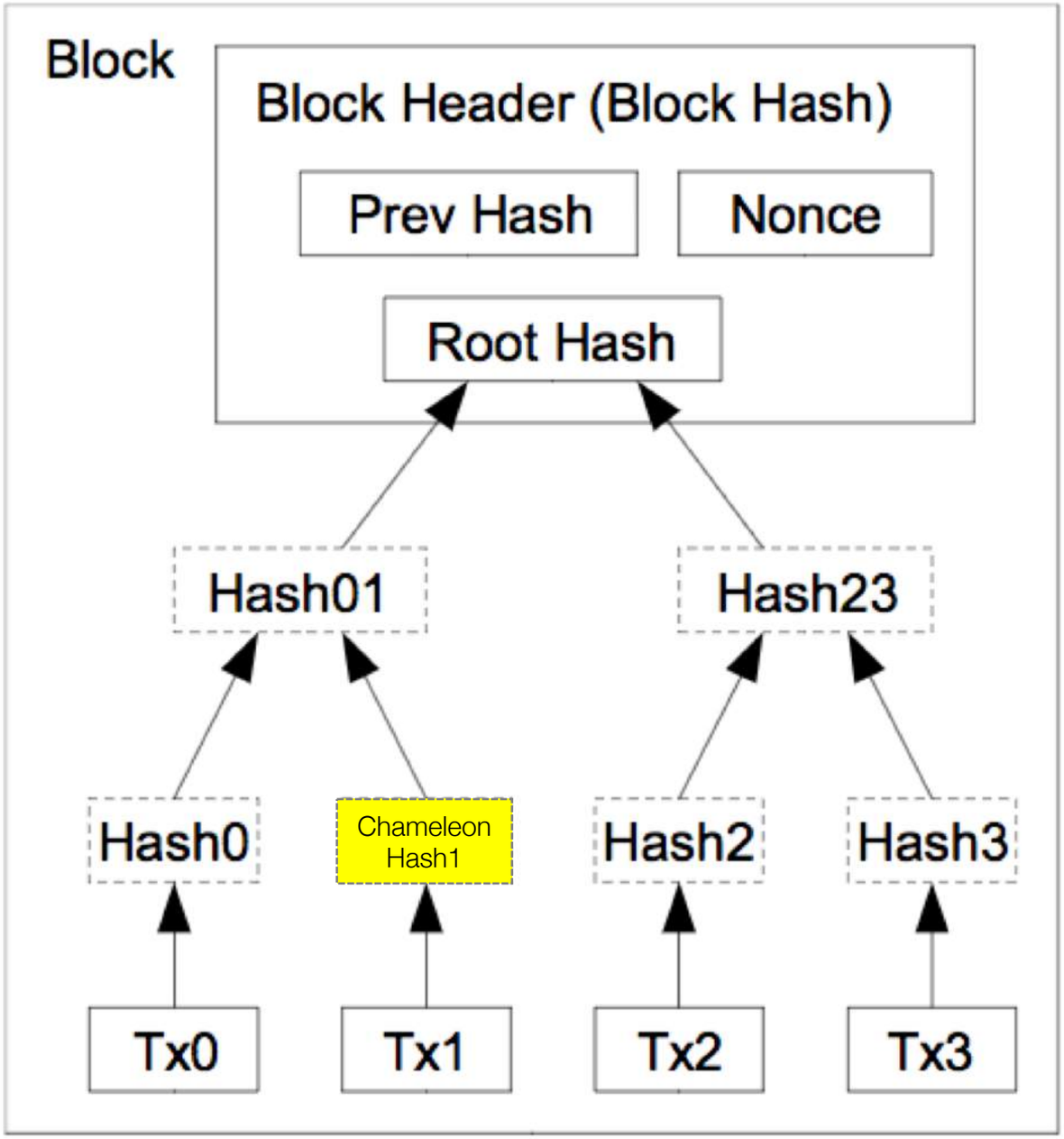
Order of Preference

- Zero-Knowledge Proof
- Hashes with secret key (peppered hashes)
- Encryption
- Hashes without additional secret key
- Clear text

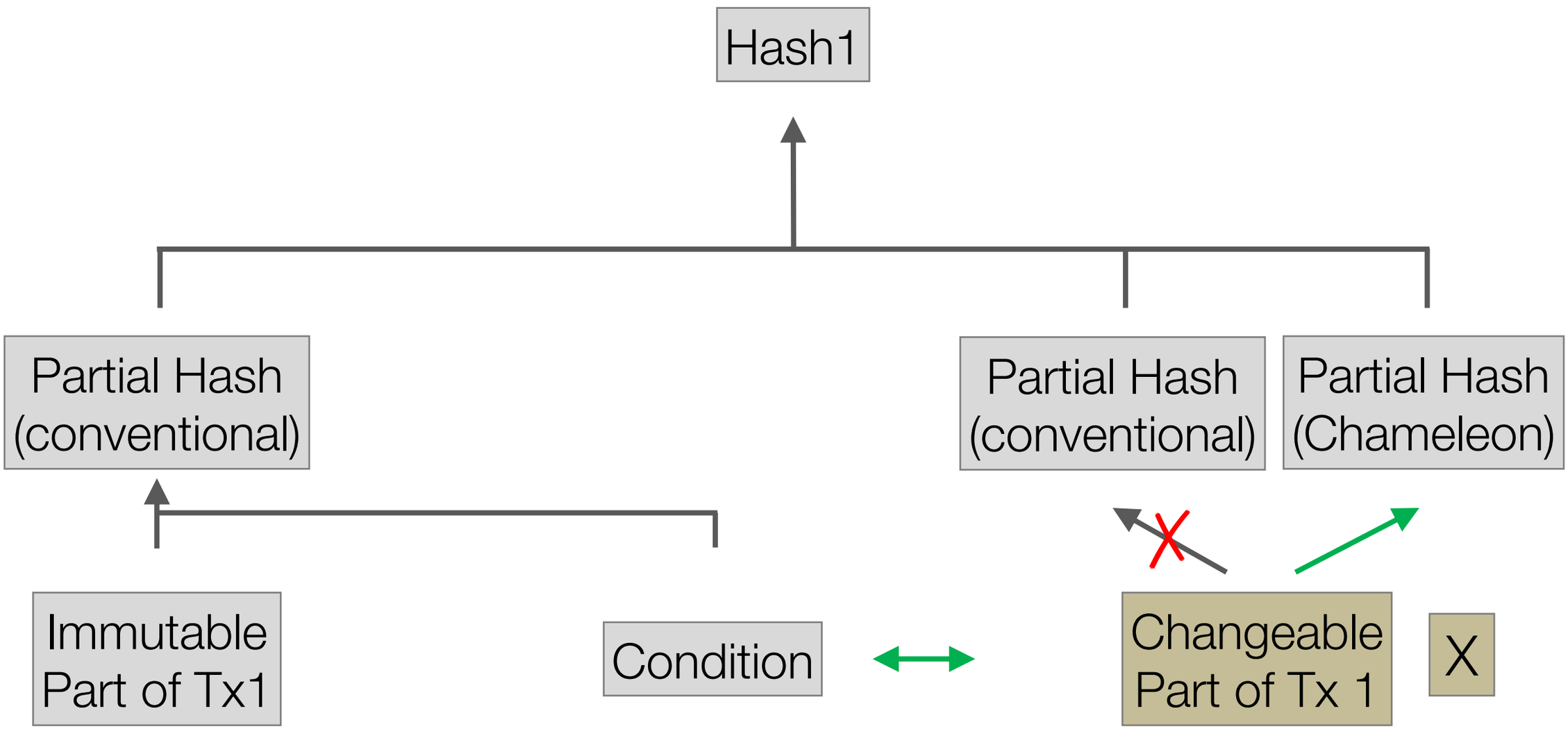
Chameleon Hash Functions

- Hash functions that can be reversed with a private key
- Enables modifiable blockchains
- Modification remains visible
- Modification can be subject to conditions
- Modification should be limited to specific parts of a transaction

Chameleon Hash Functions



Chameleon Hashfunctions



When to Use Chameleon Hash Functions?

- Some part of the data on a blockchain should stay immutable
- Another part of the data shall be deleted or changed after a certain time under specific conditions
- It is known in advance, what part of the data needs to be immutable and what part needs to be changeable

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)

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?

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, but only if they retain control of the smart contract

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

Public Blockchains vs. Permissioned Blockchains

Public Blockchains

- ! Who sends and signs a transaction is a controller
- ? Anonymity
- ? Processing agreements
- ? Liability

Permissioned Blockchains

- ! Who attributes permissions is controller
- ! Processing agreements
- ! Liability
- ? Joint controller

Blockchain

GDPR Quick Check

beta test V0.2

https://erbguth.ch/QuickCheck

Thank you for your attention!

Questions?