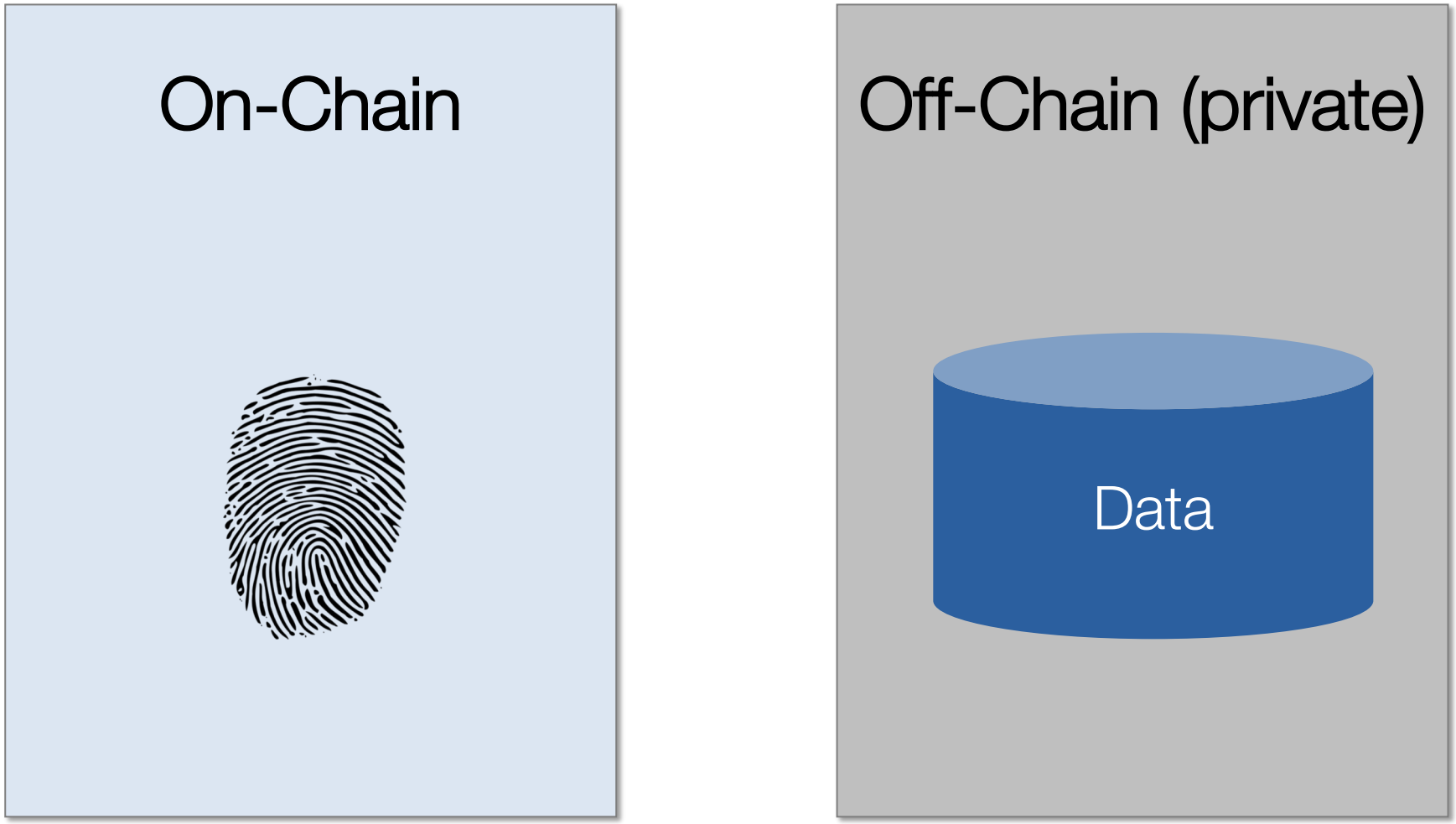
GDPR-Compliant Hashing

University of Geneva, April 8, 2019
Jörn Erbguth, Dipl.-Inf., Dipl.-Jur.
Consultant Legal Tech, Blockchain, Smart Contracts and Data Protection
Lecturer at the University of Geneva and Geneva School of Diplomacy

joern@erbguth.ch +41 787256027

UNIVERSITÉ DE GENÈVE

GDPR-Compliant Hashing



Cryptographic hash functions

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

Demo 2

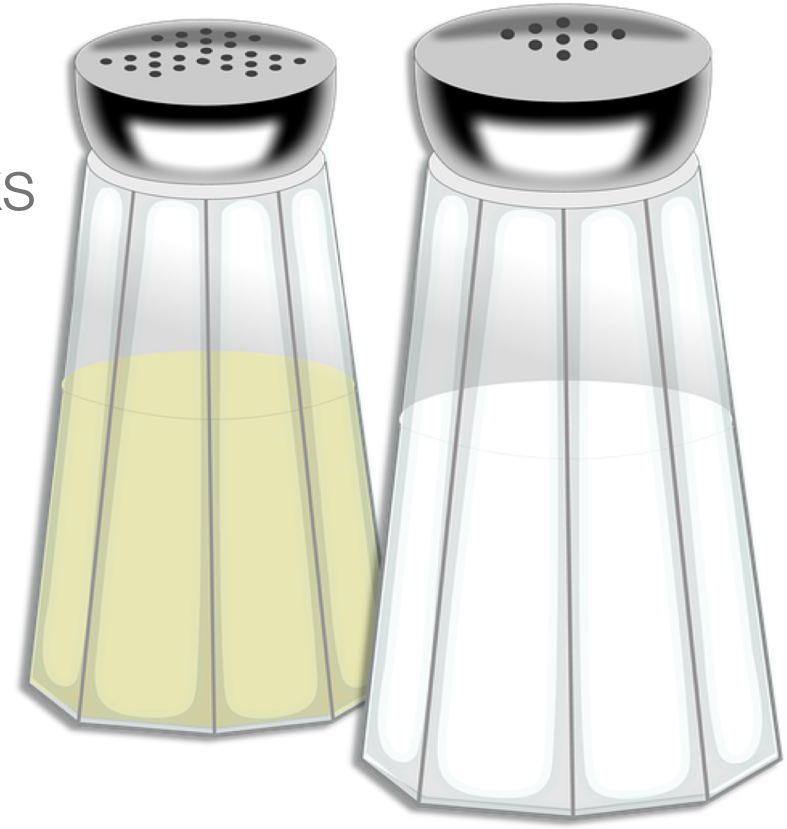
Use Cases for Cryptographic Hash Functions

- 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!

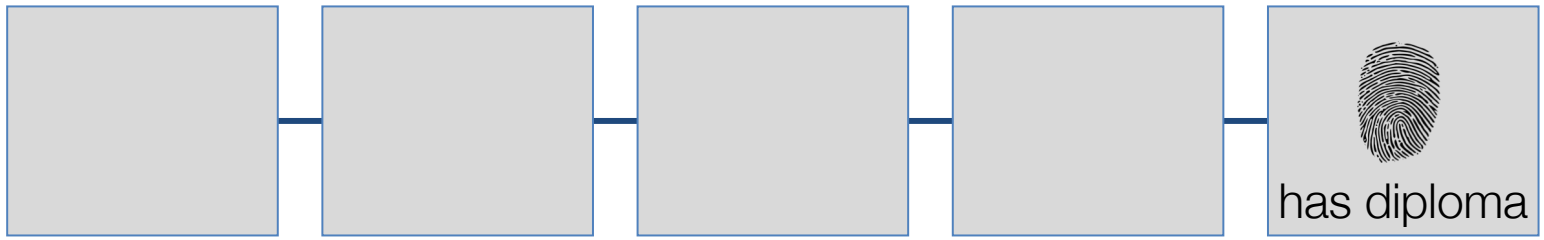
Adding Salt and Pepper to Hashes

- Ensuring enough **entropy**
- Making guessing really hard
- Can prevent rainbow table attacks
- Can prevent parallel attacks



Kryptographic Hashing – GDPR-Compliant

Kryptographic Hashing – not GDPR-Compliant



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	→	8762764826745926530869 7
Lisa	Doe	98793603485743636365	→	98796983579348569273643

On-chain

Hash	Article	Quantity	Price
8762764826745926530869 7	1984 by George Orwell	1	10
98796983579348569273643	Ulysses by James Joyce	1	20
8762764826745926530869 7	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	→ 7648265467265308697 4532
Lisa	Doe	Ulysses by James Joyce	1	98793603485743636365	→ 35793485692736433524132
John	Smith	Inside Wikileaks by Domscheit-Berg	1	29749850385739857395	→ 86786876868594939653656

On-chain

Hash	Price
7648265467265308697 4532	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

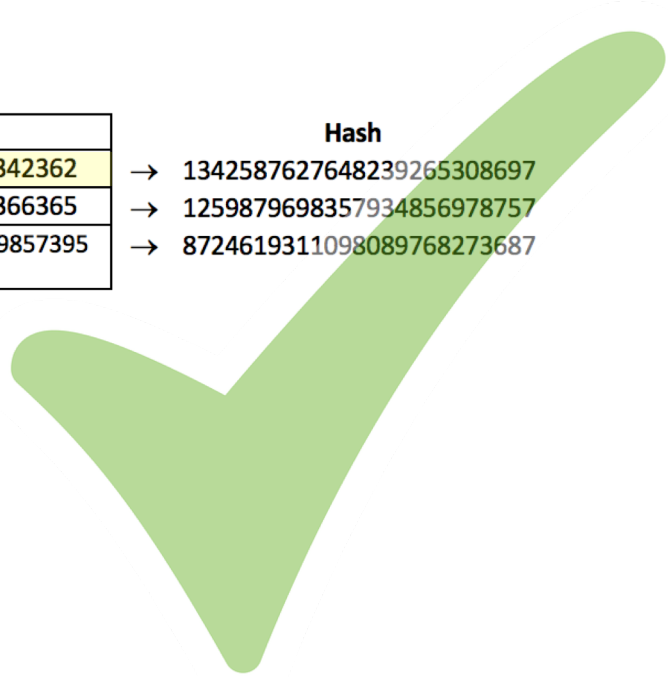
Off-chain

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

Hash	
→	134258762764823926530869 7
→	125987969835793485697875 7
→	872461931109808976827368 7

On-chain

Hash
134258762764823926530869 7
125987969835793485697875 7
872461931109808976827368 7



How to Hash Data

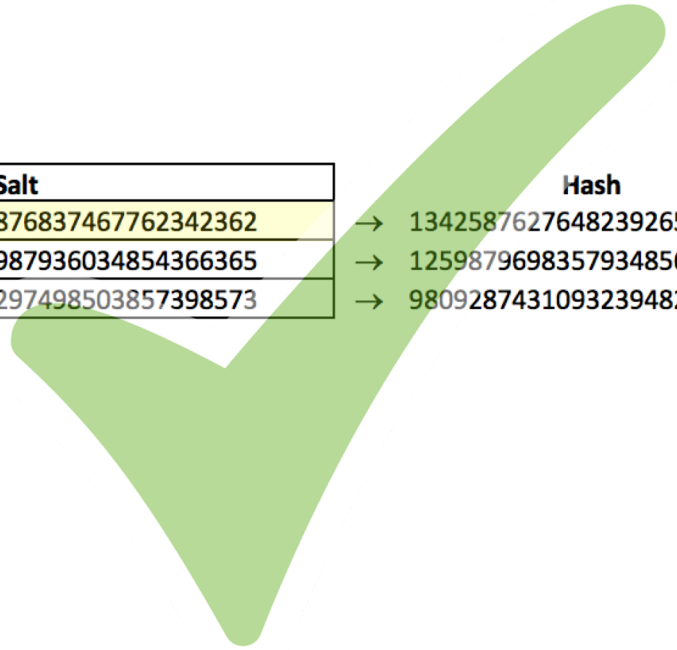
Data

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
134258762764823926530869 7	10
125987969835793485697875 7	20
980928743109323948235789 8	15

Test: Can you Derive Personal Data from the Blockchain?

Does the blockchain disclose personal data?

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?


Blockchain
GDPR Quick Check
beta test V0.2
https://erbguth.ch/QuickCheck