



Blockchain and GDPR

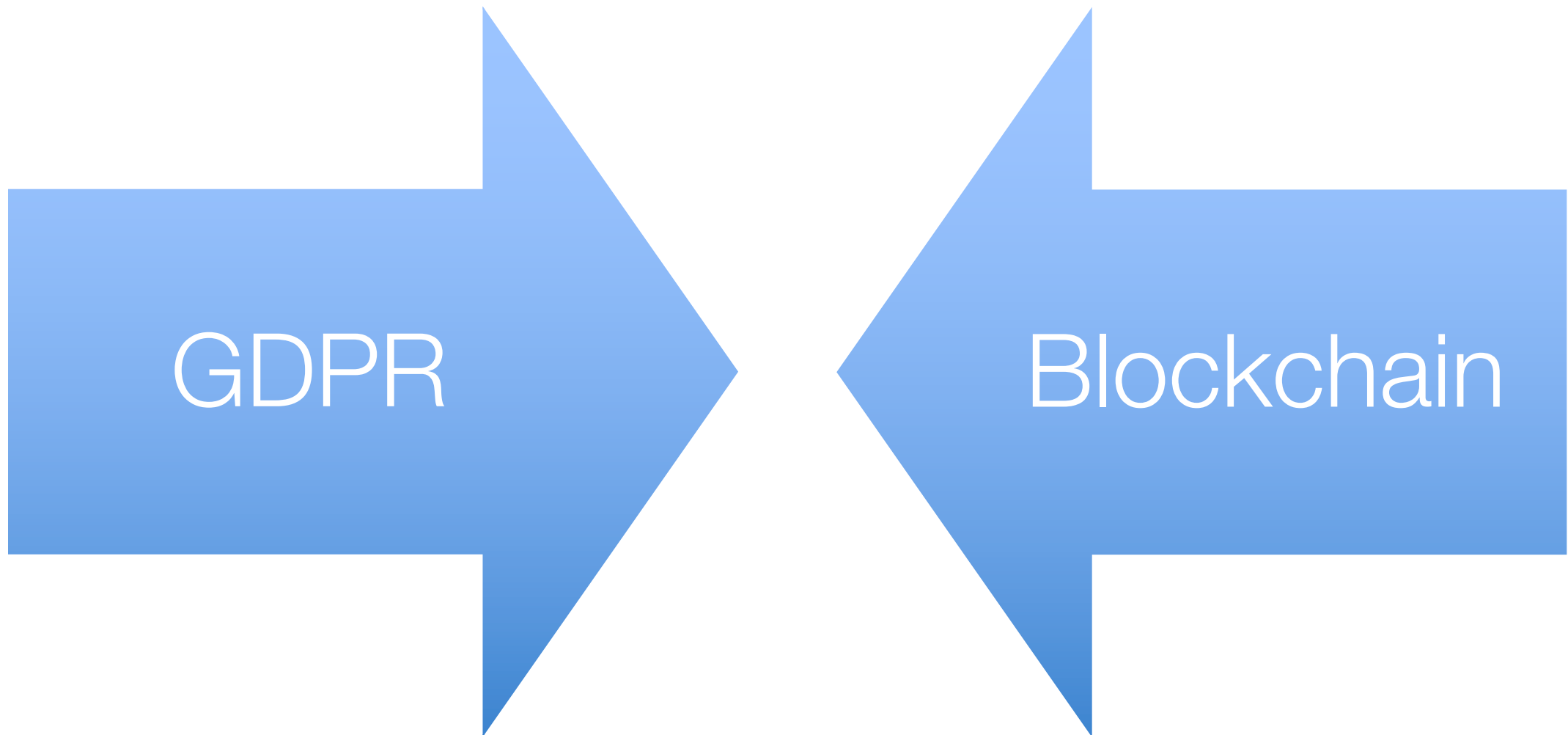
Blockchain & Bitcoin Conference, Geneva, October 9, 2018

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 ...

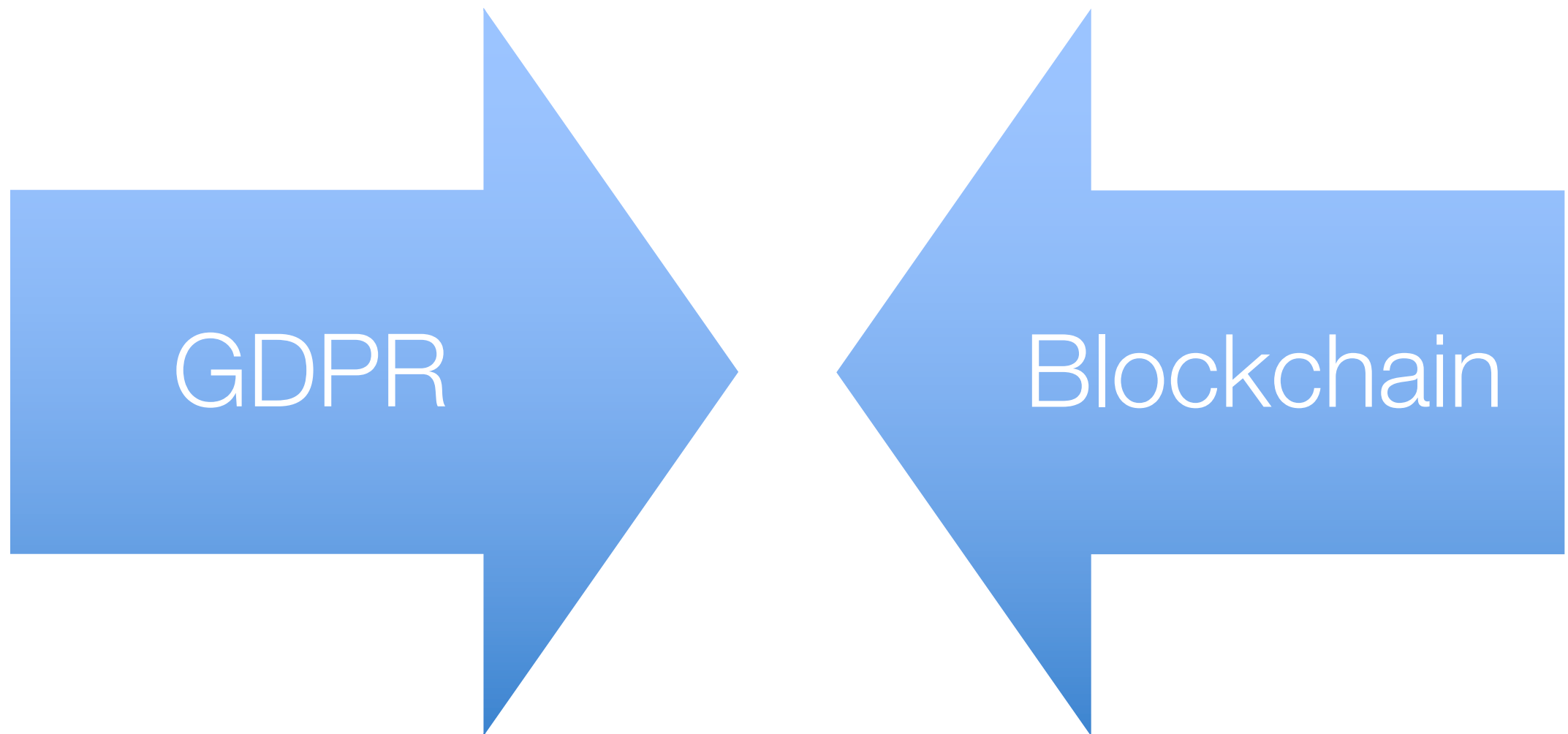
Art. 16: rectification

Art. 17: erasure

Art. 18: restriction of processing

immutable
public

GDPR vs. Blockchain



Clear responsibility
controller
processor

distributed responsibility
anonymous participation

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.

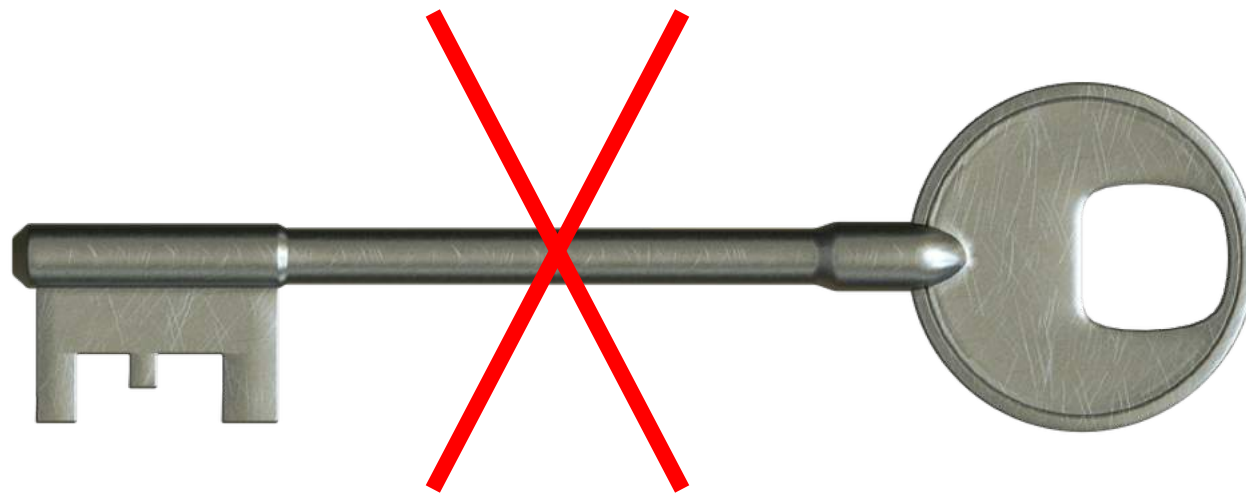
Examples of personal data

- ✓ IP addresses
- ✓ Bitcoin addresses
- ✓ “anonymized” movement profile
- ✓ “anonymized” browsing history
- x aggregated movement profiles
- x aggregated browsing history

Note: Look at the individual case – do not generalize

Encryption

Deletion of the encryption key = deletion of the content?



SAMSUNG

WARRANTY VOID IF REMOVED

MMCQE28GFMUP – MVA



DFK300A842 – SE842A0588



Model : Slim 128GB uSATA MLC

SSD P/N : MMCQE28GFMUP – MVA

0842

REV 0

F/W VAM05S1Q

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.

이 제품은 민감한 전자 부품이 포함되어 있으므로 충격이나 진동에 주의하십시오. 회로에 손을 대면 고장나거나 보증이 무효가 됩니다. Product of KOREA



1. 모델명: Slim 128GB uSATA MLC
2. 제조사: SEC - M - SLIM28GUSATA(B)



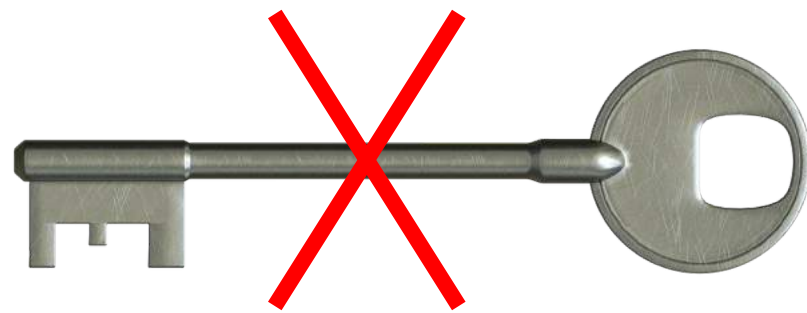
3. 제조일자: 2008.10.07
4. 제조사: 삼성전자가
5. 제조사/모델명: 삼성전자가 / 삼성전자가



SAMSUNG
MMCQE28GFMUP – MVA

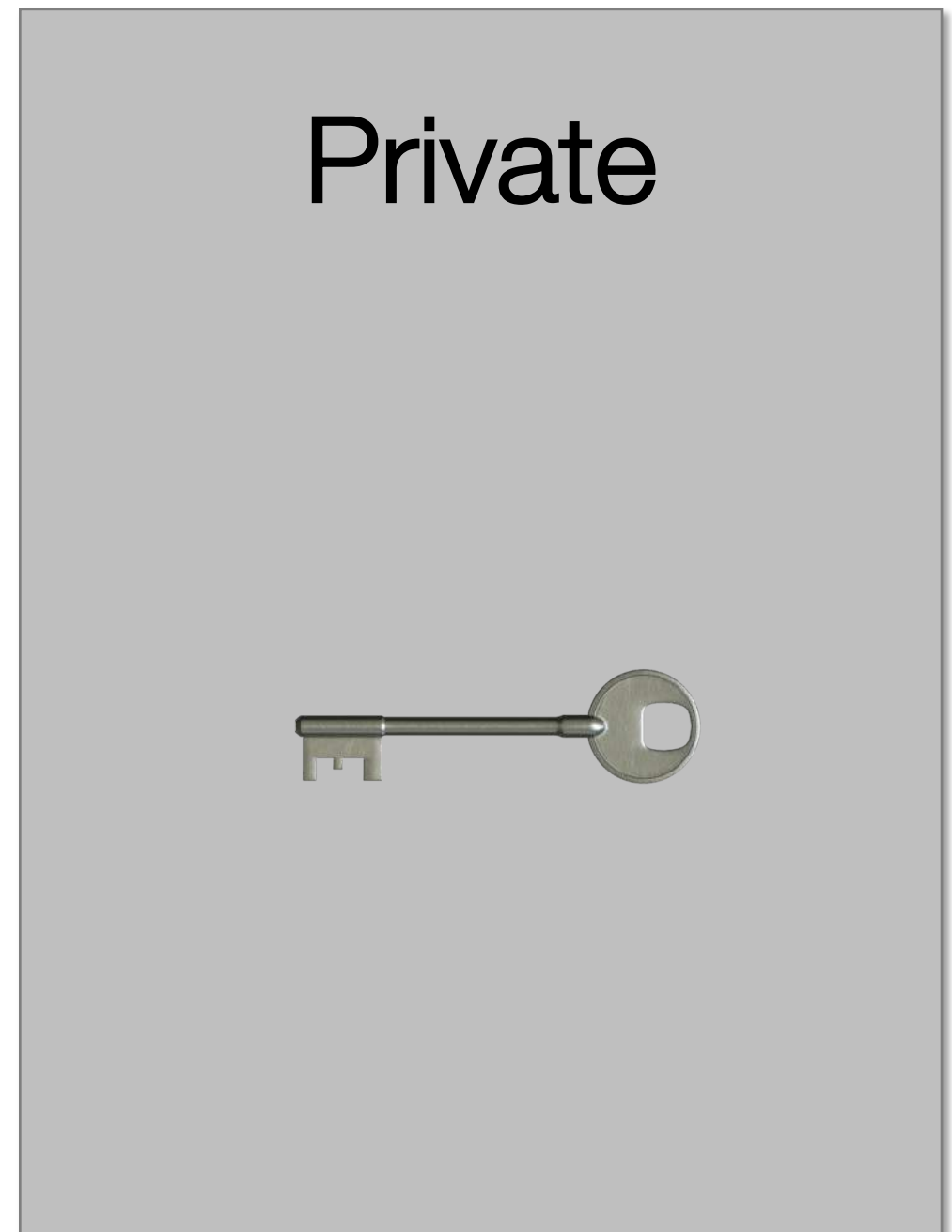
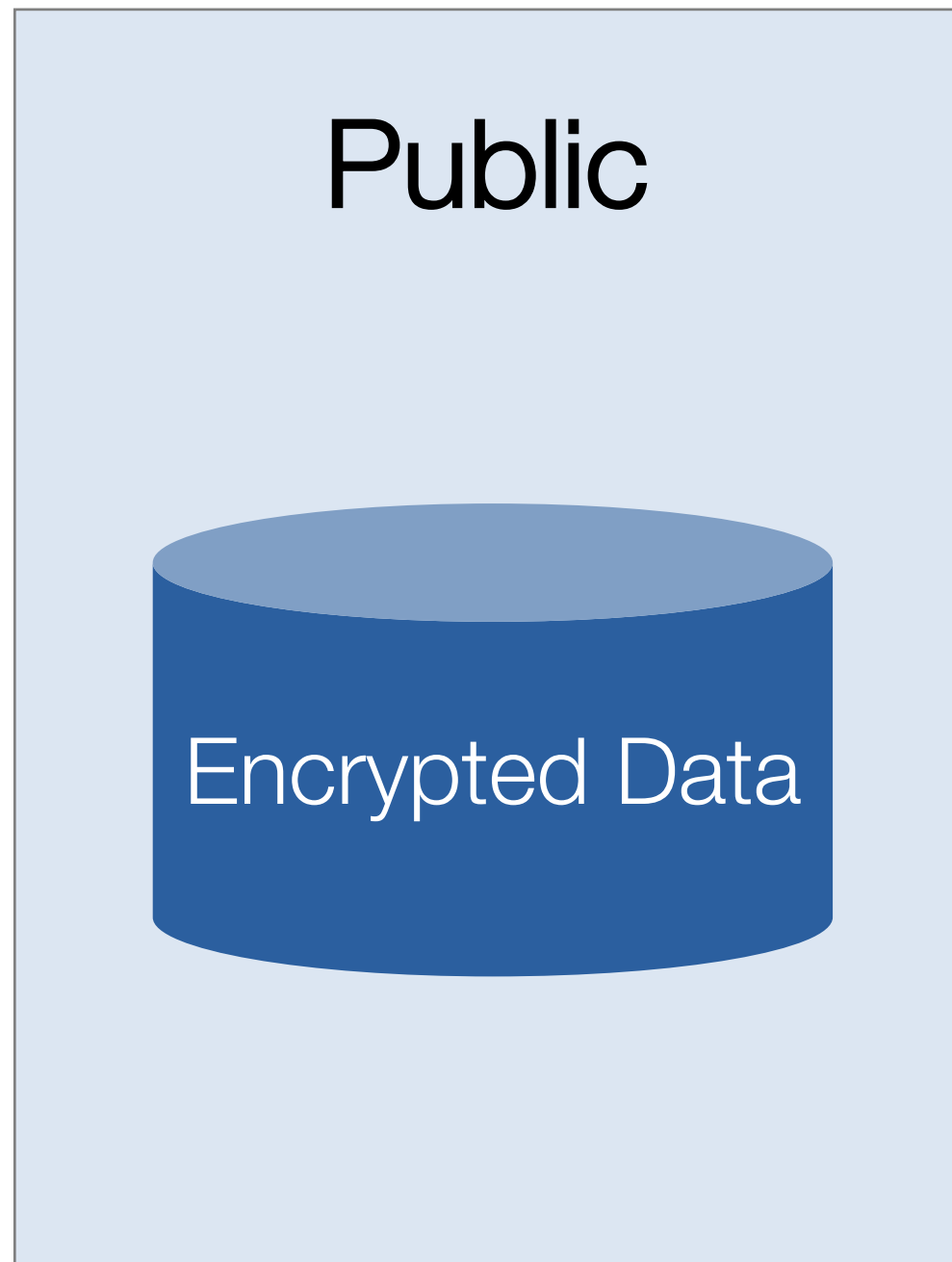
GDPR-compliant deletion?

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

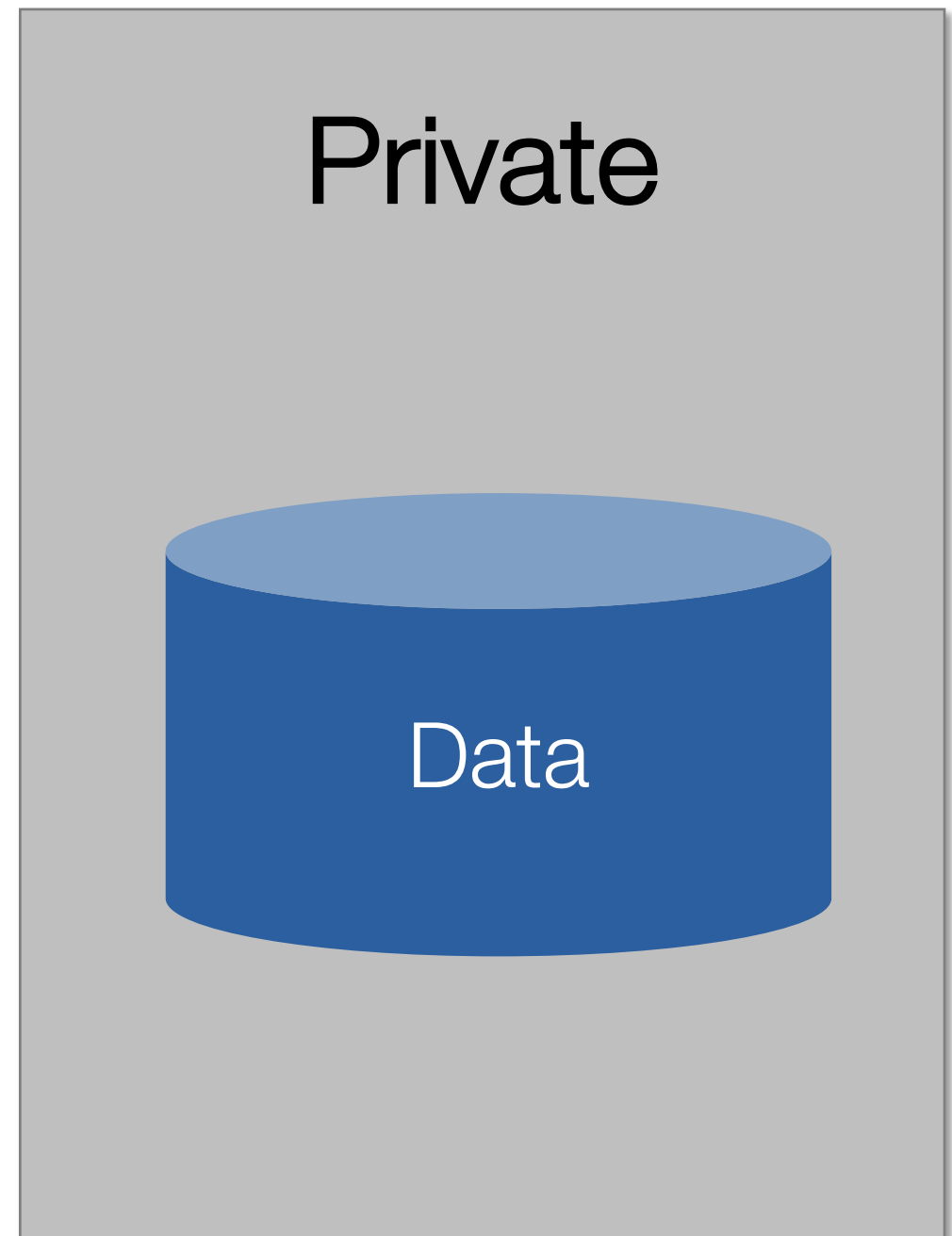


- Is there a remaining copy of the key?
- Will the encryption method become insecure in the future?

Hash value as a better alternative to encryption



Hash value as a better alternative to encryption



Cryptographic hash functions

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



Examples of cryptographic hashes

- Switzerland

2275583196D791405892AACA0D87743C872F3FC0CF3308A6C3EF82528918AA8A

- Switzerland.

43CF6F3ECA7253FFAB1FD5104172280189B91FDD5FA26774FCA6475FFA1E2EC9

-

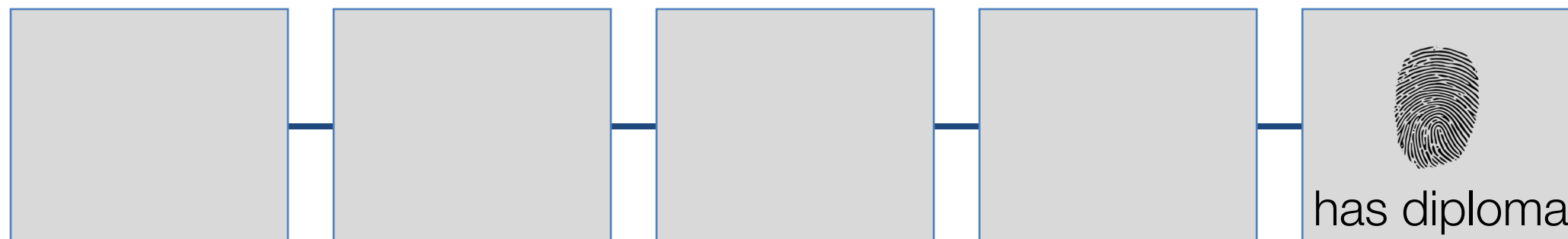


8C4B4C4E211BA8C1A62DE2A3A6CA5AC8BFF501C14410100DD90D5077A0AC061E

GDPR-compliant use of hash values



Non-GDPR-compliant use of hash values



Use cases for cryptographic hash functions

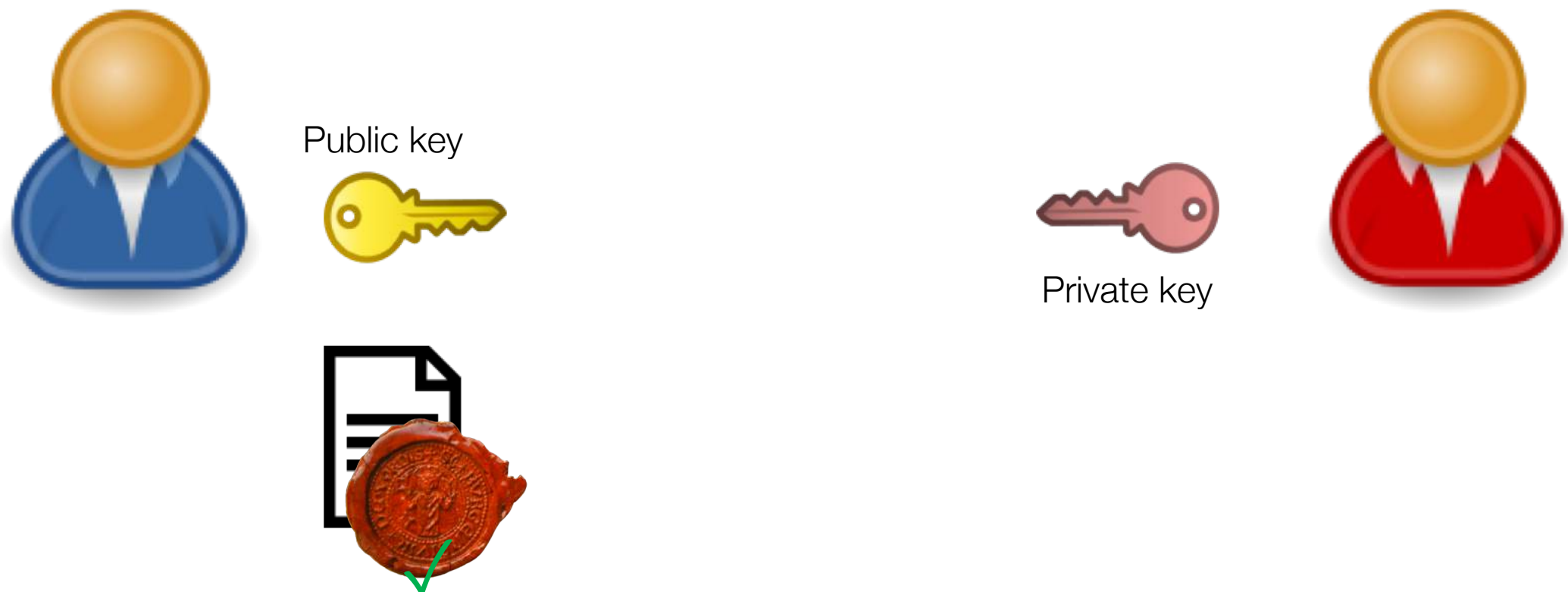
- Validate external documents
- Time-stamping
- Proof of Existence
- Basic functionality for cryptography and DLT

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

Zero-Knowledge Proof

Proof of knowing something
without revealing it

Simple Zero-Knowledge Proof



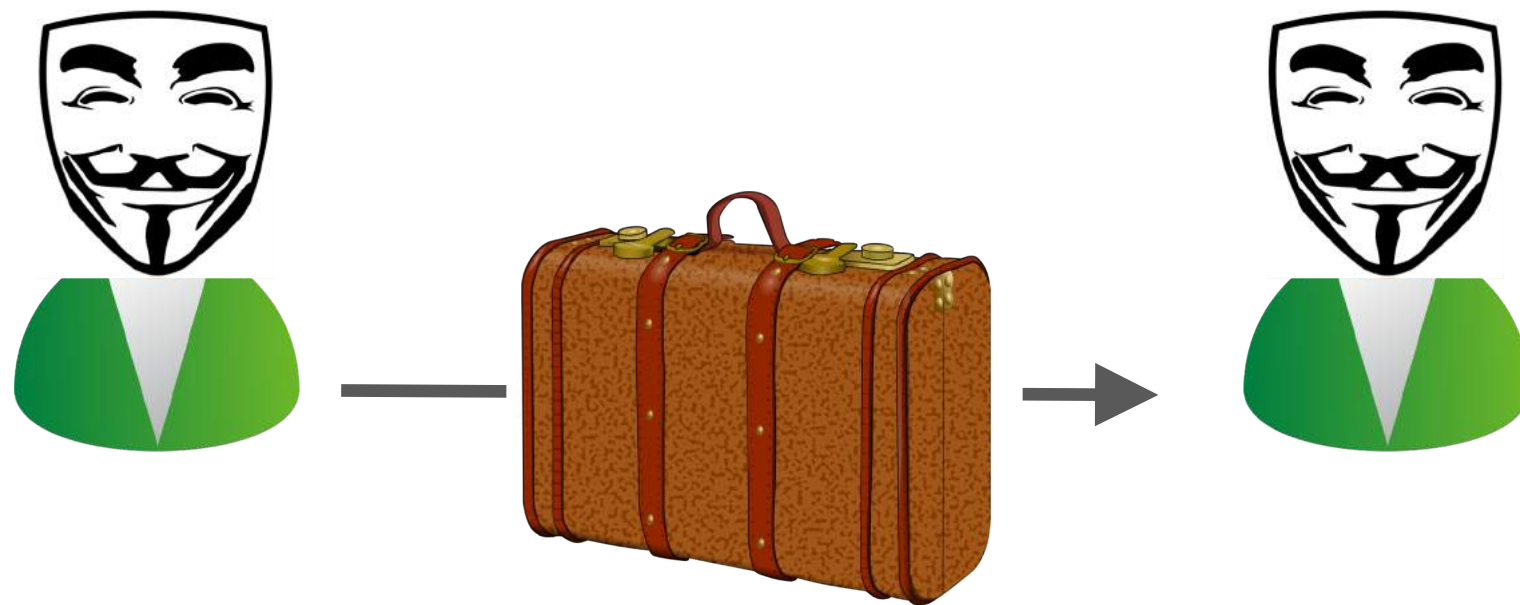
Zero-Knowledge Proof – example



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

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


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 

Duties of controllers and processors

- 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

Blockchain

GDPR Quick Check
beta test V0.2



<https://erbguth.ch/QuickCheck>

How to Learn More?

*Certificate of Advanced Studies (CAS)
on Decentralized Applications (dApps)
Development with Blockchains and
Distributed Ledger Technologies (DLT)*

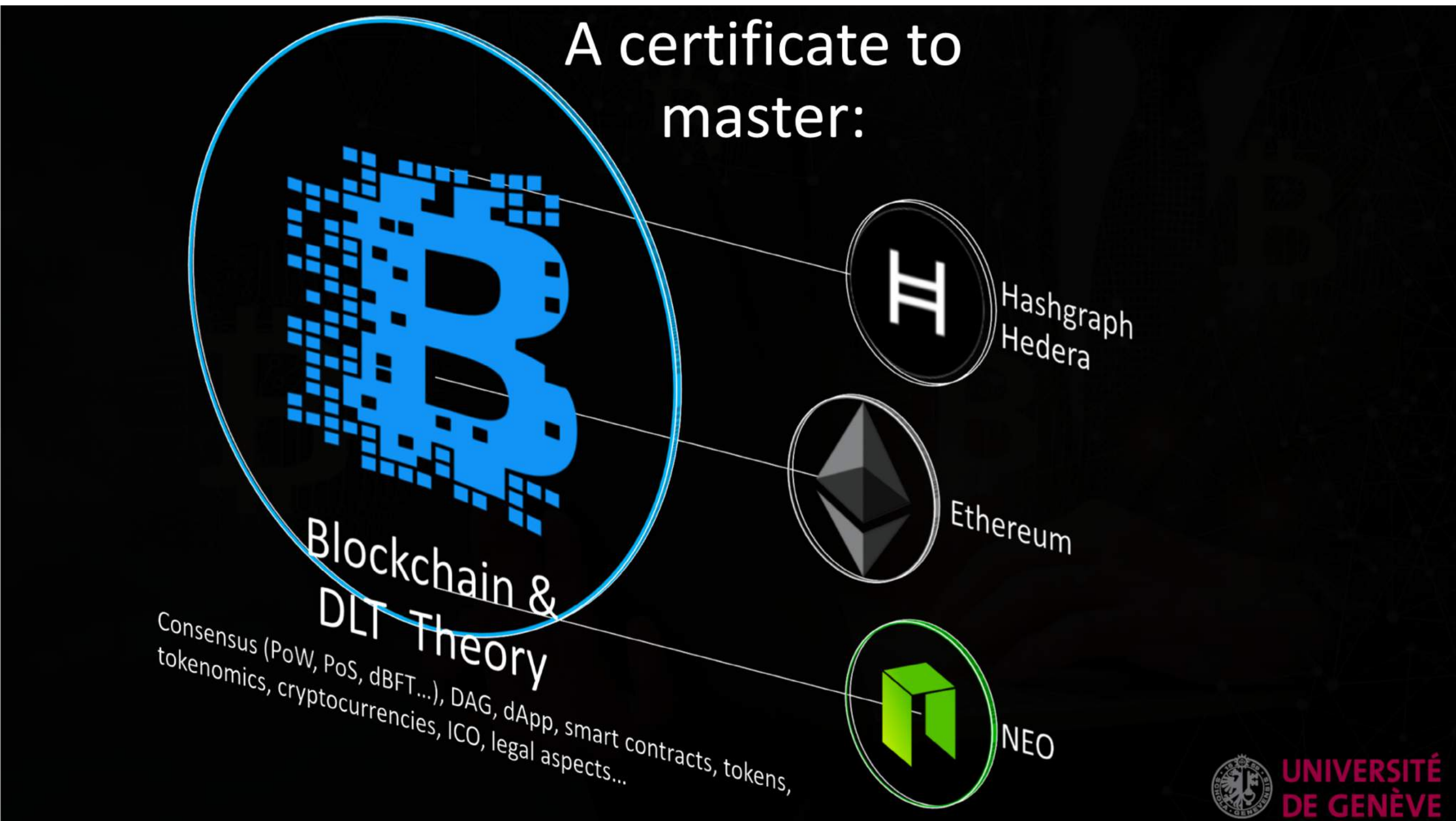


**UNIVERSITÉ
DE GENÈVE**

Dr. Jean-Marc Seigneur, Director
Jean-Marc.Seigneur@unige.ch

<https://www.cas-blockchain-certification.com>

How to Learn More?



How Does Geneva Support You?



REPUBLIC AND STATE OF GENEVA
Department of Security
Directorate General for Economic Development, Research and Innovation

Guide:

Initial Coin Offerings (ICOs) in the Canton of Geneva

27 September 2018 Edition

How Does Geneva Support You?



Geneva ICO evaluation request

English

Contact person or representative

You are :

☐ (co-)founder

☐ advisor

☐ employee

Name

Given name

Thank you for your attention!

Questions?