WORLD SUMMIT ON THE INFORMATION SOCIETY

WSIS Forum 2019

Blockchain & Data Protection

Jörn Erbguth
Consultant on Blockchain & GDPR

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

GDPR Quick Check
https://erbguth.ch/QuickCheck

UNIVERSITÉ DE GENÈVE

ITU

What is the **b**iggest **t**hreat to our **p**rivacy?

Data is stored in different locations
Blockchain ensures data is not manipulated

Zero-knowledge proofs, ring signatures …

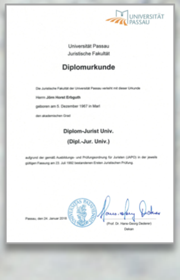
? Can blockchain foster privacy? ✓

? Right to be forgotten! ✓

Data is stored in different locations

Blockchain ensures data is not manipulated

Zero-knowledge proofs, ring signatures …



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

UNIVERSITAS PATAVIENSIS

(Prof. Dr. Hans-Georg Dederer)
Dekan

Jörn Erbguth, consulting@erbguth.ch
Blockchain & Data Protection
WSIS conference, ITU
Geneva, April 8, 2019

Better Privacy Through the Use of Blockchain

Privacy Coins

MONERO

Zcash

Self Sovereign ID

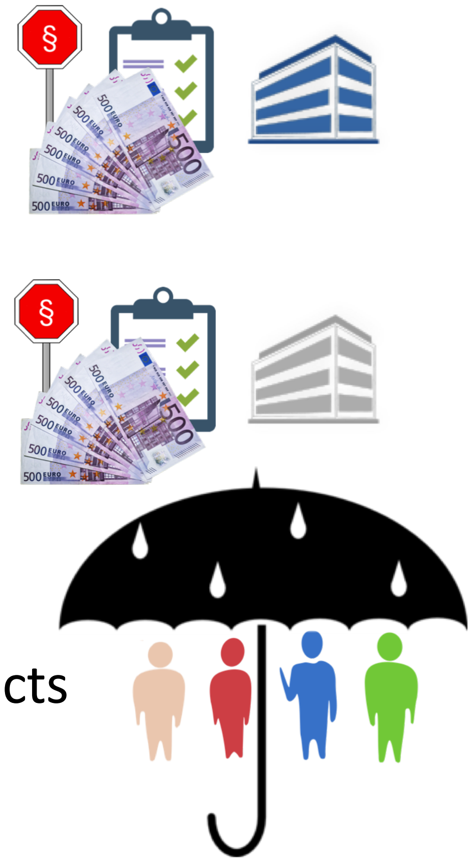
enigma

JOLOCOM

Privacy Frameworks

BLOCKSTACK

How Data Protection Regulation Works



Controller

Determines the purposes and means of processing

Processor

Processes data on behalf of the controller

Data-Subjects

WORLD SUMMIT ON THE INFORMATION SOCIETY

Blockchain is a threat to privacy?

Blockchain fosters privacy!

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

GDPR Quick Check

https://erbguth.ch/QuickCheck

UNIVERSITÉ DE GENÈVE

ITU

WORLD SUMMIT ON THE INFORMATION SOCIETY

Blockchain & Data Protection

Summary of today´s Workshop at the University of Geneva

Katrin Kirchert, LL.M.
Lawyer for Privacy and Data Protection Law

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

UNIVERSITÉ DE GENÈVE

ITU

WORLD SUMMIT ON THE INFORMATION SOCIETY

News from courts and data protection authorities that might affect blockchains

Katrin Kirchert, LL.M.

- much information about financial regulation of Blockchain
- little information regarding data protection issues

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

UNIVERSITÉ DE GENÈVE

ITU

WORLD SUMMIT ON THE INFORMATION SOCIETY

New technological developments in the blockchain space
zkSNARKs for scaling and privacy

Alexandre Poltorak

- technologies based on Zero Knowledge Proofs for higher scaling and to protect privacy
- zkSNARK = Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

UNIVERSITÉ DE GENÈVE

ITU

WORLD SUMMIT ON THE INFORMATION SOCIETY

Deletion in the context of cryptography

Christian Wirth & Michael Kolain

legal challenges and technical approaches for the right to be forgotten

WSIS FORUM 2019 10 YEAR ANNIVERSARY

UNIVERSITÉ DE GENÈVE

ITU

WORLD SUMMIT ON THE INFORMATION SOCIETY

Can encrypted data be considered to be anonymous?

Carmen de la Cruz

- encrypted personal data can always be reverse engineered according to the Regulators
- more sophisticated encryption techniques used to anonymize personal data (stealth addresses, Zero Knowledge Proofs) are necessary and/or a change of the Regulation

WORLD SUMMIT ON THE INFORMATION SOCIETY

GDPR-compliant use of hashing

Jörn Erbguth

Hashing can provide true privacy, but you have to apply it the right way

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

UNIVERSITÉ DE GENÈVE

ITU

WORLD SUMMIT ON THE INFORMATION SOCIETY

Who is controller of the processing of a smart contract?

Gabriel Jaccard

- system of blockchain was not built to be GDPR-compliant
- new principles of governance are necessary to make lawful use of smart contracts

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

UNIVERSITÉ DE GENÈVE

ITU

Conclusions

1. Do not put any personal data (at all) on a blockchain.
2. Use Privacy Enhancing Technology and ensure that no personal data can be derived from the blockchain.
3. Obtain a justification that is permanent. Don´t rely only on consent!
4. Let users put the data on a public blockchain themselves.
5. Build specialized blockchains that forget.

Standards for Blockchain and Distributed Ledger Technology

Martin Adolph

ITU Telecommunication Standardization Bureau

April 2019

Blockchain and DLT – ITU portfolio

ITU-T Focus Groups

Pre-standardization

- **Application of DLT (FG DLT) -** identifies use cases, works on terminology, a high-level architecture, an assessment framework, and regulatory aspects
- **Digital Fiat Currency (FG DFC)** - explores blockchain as enabler for CBDC
- **Data Processing and Management to support IoT and Smart Cities & Communities (FG DPM)** - studies use of blockchain in this context

Open to non-members

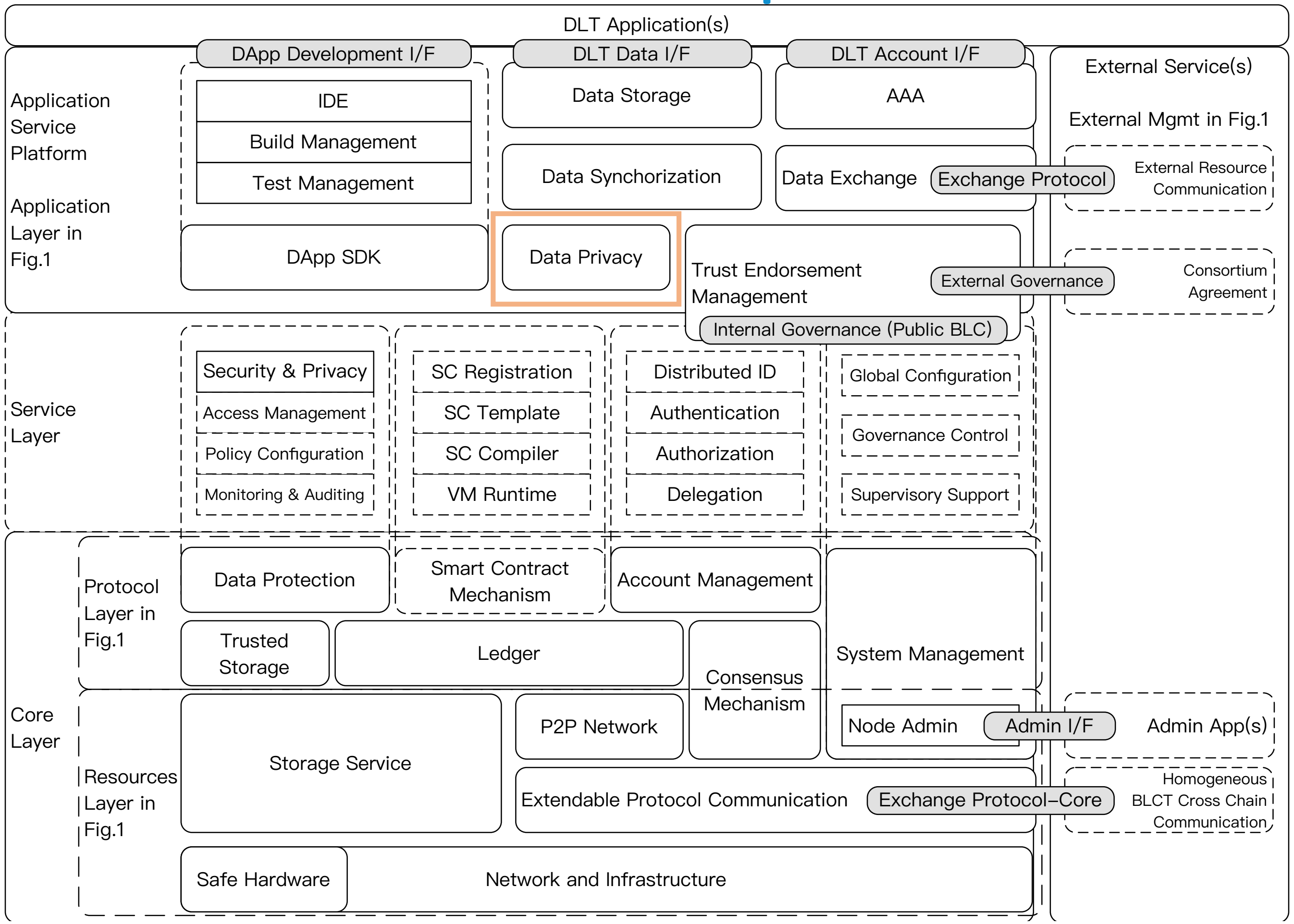
ITU-T Study Groups

Formal standardization

- **SG13** - Cloud computing requirements for blockchain as a service (BaaS); blockchain in NGNe (2 work items)
- **SG16** - DLT and e-services (Question 22/16) (4 work items)
- **SG17** - Security aspects for DLT (Question 14/17: 10 work items)
- **SG20** - “Blockchain of things” (4 work items)

ITU members only

Focus Group on Application of DLT (FG DLT) – **DLT architecture and platform assessment criteria**



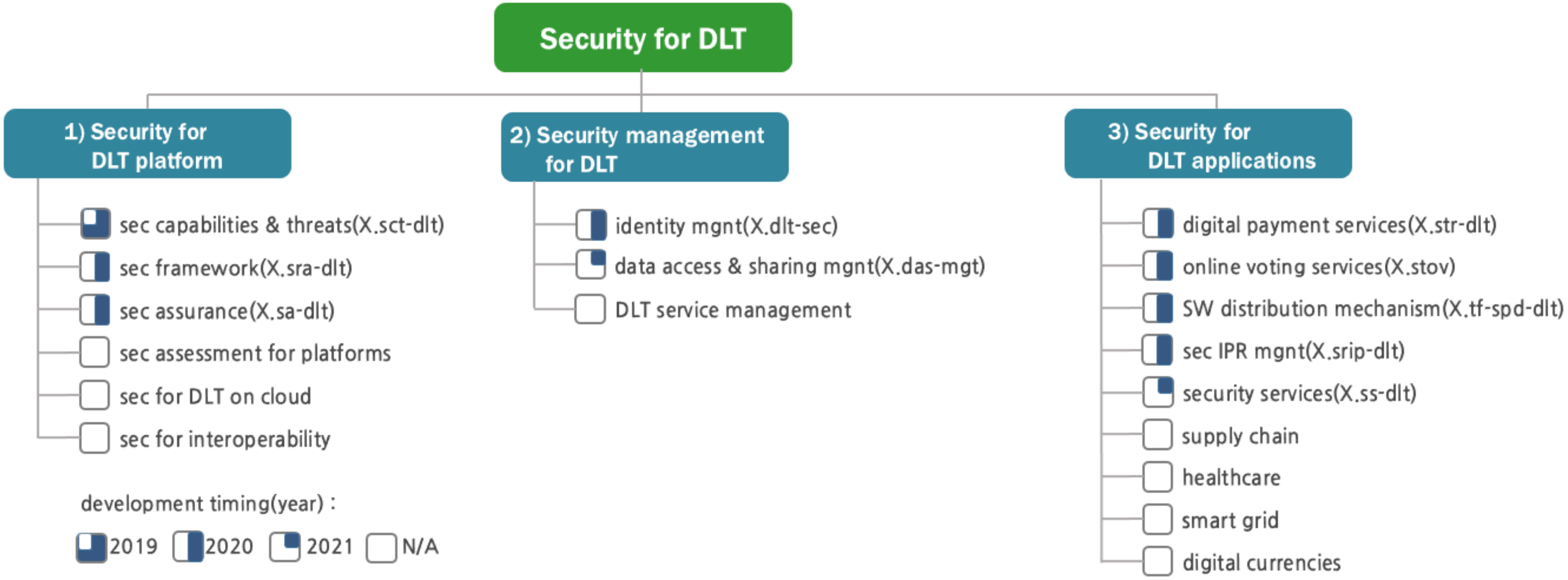
- 7 Criteria for DLT application functions
  - 7.4 Data privacy
    - 7.4.1 Secure transmission
    - 7.4.2 Restricted data access
    - 7.4.3 Privacy protection

Focus Group on Application of DLT (FG DLT) – Regulatory framework

DLT key features	Regulatory aspects include
Distributed	Human right vs. limitation of rights; Within and beyond system boundaries; Interoperability rules
Tamper-evident and -resistant	Measurement, correction, or removal of DLT data
Shared	Scalability: Data Integrity (accuracy), Privacy (data usage), Anti-trust, Confidentiality (access). Rules: Continuous audit for adherence & enforcement
Incentive- and asset-based	Digital Virtual & Digital Fiat Currencies. Tokens.
Open and transparent	Regulation: sector (e.g., financial) or country (law)
Anonymous	AML & KYC statutes vs. Data protection laws
Autonomous	Governance-less vs. self-governance

Goal: Provide guidance to policy makers, regulators.

Study Group 17 – Security aspects for DLT



Security for DLT

1) Security for DLT platform

- ■ sec capabilities & threats(X.sct-dlt)
- ◨ sec framework(X.sra-dlt)
- ◨ sec assurance(X.sa-dlt)
- □ sec assessment for platforms
- □ sec for DLT on cloud
- □ sec for interoperability

2) Security management for DLT

- ◨ identity mgnt(X.dlt-sec)
- ◳ data access & sharing mgnt(X.das-mgt)
- □ DLT service management

3) Security for DLT applications

- ◨ digital payment services(X.str-dlt)
- ◨ online voting services(X.stov)
- ◨ SW distribution mechanism(X.tf-spd-dlt)
- ◨ sec IPR mgnt(X.srip-dlt)
- ◳ security services(X.ss-dlt)
- □ supply chain
- □ healthcare
- □ smart grid
- □ digital currencies

development timing(year) :

■2019 ◨2020 ◳2021 □N/A

ISO work on blockchain and DLT – **ISO/TC 307**

WG	Title	Work Items	
1	Foundations	…	
2	**Security, privacy and identity**	ISO/NP TR 23576	Security management of digital asset custodians
		Study item	Security Evaluation of Consensus Models
2&3		Study item	Security Issues of Smart Contracts
3	Smart contracts and their applications	…	
4	**JWG (Joint working group between TC307 and ISO/IEC JTC1 SC27 “IT Security techniques”)**	ISO/NP TR 23244	**Privacy and personally identifiable information protection considerations**
		ISO/NP TR 23245	Security risks, threats and vulnerabilities
		ISO/NP TR 23246	Overview of identity management using blockchain and DLT
5	Governance	…	

Find out more at https://itu.int/en/ITU-T/focusgroups/dlt/

WORLD SUMMIT ON THE INFORMATION SOCIETY

DIN SPEC 4997
Privacy by Blockchain Design

A standardised model for processing personal data using blockchain technology

- What's a DIN SPEC?
- To be published in December 2019
- Broad range of stakeholders

Anja Grafenauer
info@privacybyblockchaindesign.com

WORLD SUMMIT ON THE INFORMATION SOCIETY

DIN SPEC 4997
Privacy by Blockchain Design

- Common language between Law and IT
- Reduced legal uncertainty for blockchain
- Guidelines & best practices
- Foundation for further standards & regulation
- Blockchain for data sovereignty

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

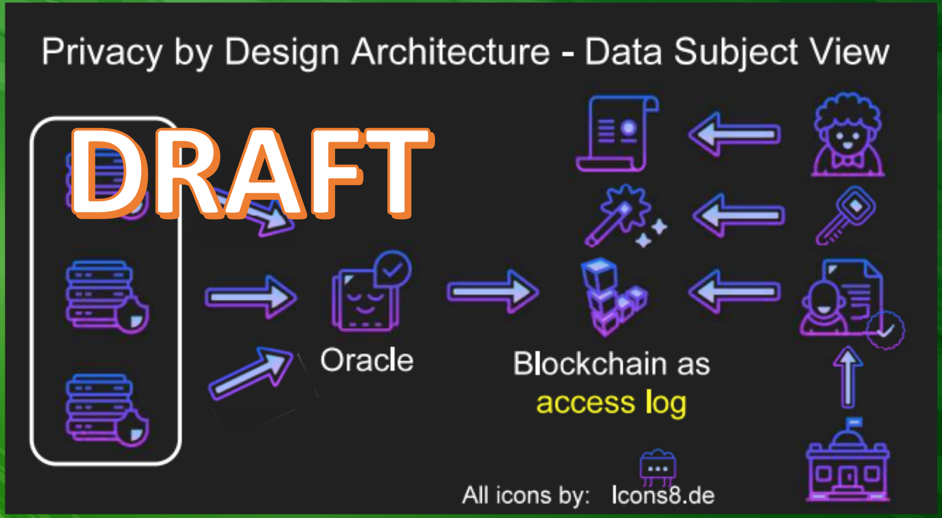
Anja Grafenauer
info@privacybyblockchaindesign.com

ITU

WORLD SUMMIT ON THE INFORMATION SOCIETY

DIN SPEC 4997

“Privacy by design” (art. 25 GDPR)
→ design patterns derived from law



Privacy by Design Architecture - Data Subject View

DRAFT

Oracle

Blockchain as access log

All icons by: Icons8.de

Anja Grafenauer
info@privacybyblockchaindesign.com

WORLD SUMMIT ON THE INFORMATION SOCIETY

Discussion

How can blockchain foster privacy?

WSIS FORUM 2019 | 10 YEAR ANNIVERSARY

GDPR Quick Check
https://erbguth.ch/QuickCheck

UNIVERSITÉ DE GENÈVE

ITU