Blockchain und GDPR

Webinar Weblaw
6. Juni 2019

Jörn Erbguth, Dipl.-Inf., Dipl.-Jur.
Berater Legal Tech, Blockchain, Smart Contracts und Datenschutz

joern@erbguth.ch +41 787256027

Blockchain

DSGVO ⇔ Blockchain

- Anwendbarkeit
- Problem Unveränderlichkeit
- Datenschutz durch Technikgestaltung
- Verantwortliche und Auftragsverarbeiter
- Haushaltsausnahme
- Rechtfertigungen
- Automatisierte Entscheidungen
- Datentransfer in Drittstaaten

Ist die DSGVO anwendbar? (Art. 2, 3)

- Ein Verantwortlicher oder Auftragsverarbeiter ist in der EU
- Anbieten von Waren oder Dienstleistungen in der EU
- Das Verhalten von Personen in der EU beobachten

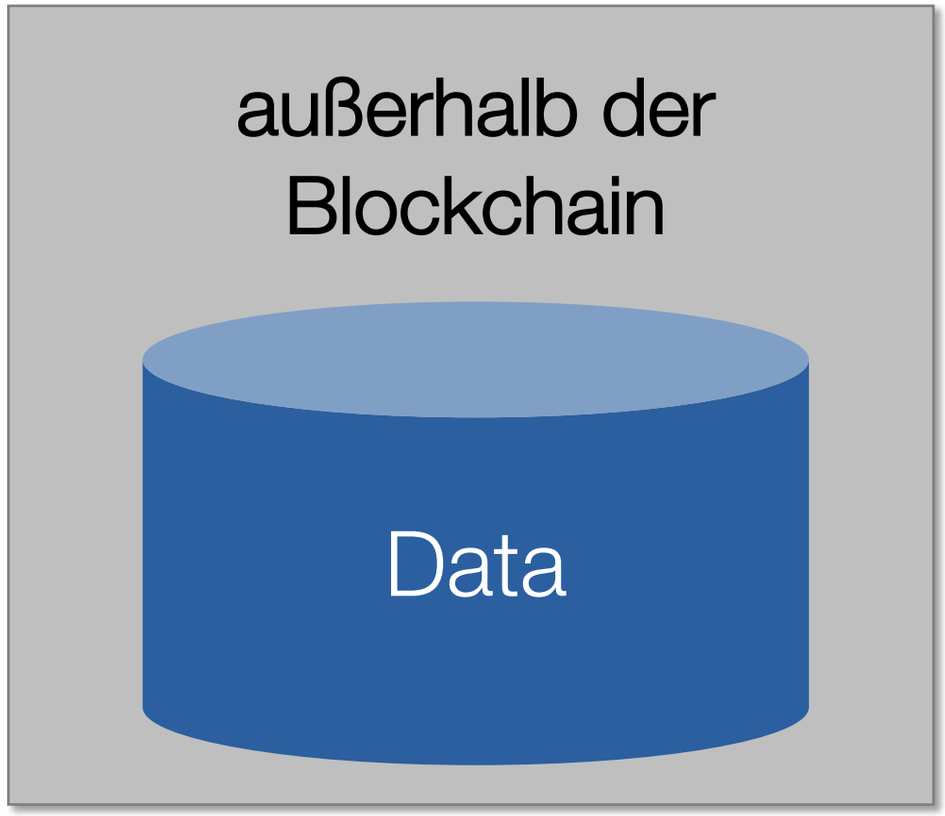
- Verarbeitung personenbezogener Daten
- Ausgenommen ist Datenverarbeitung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten

Unveränderlichkeit

- Recht auf
  - Art. 16: Berichtigung
  - Art. 17: Löschen / Vergessen werden
  - Art. 18: Einschränkung der Verarbeitung

⇒ Ablage personenbezogener Daten nur bei dauerhafter Berechtigung

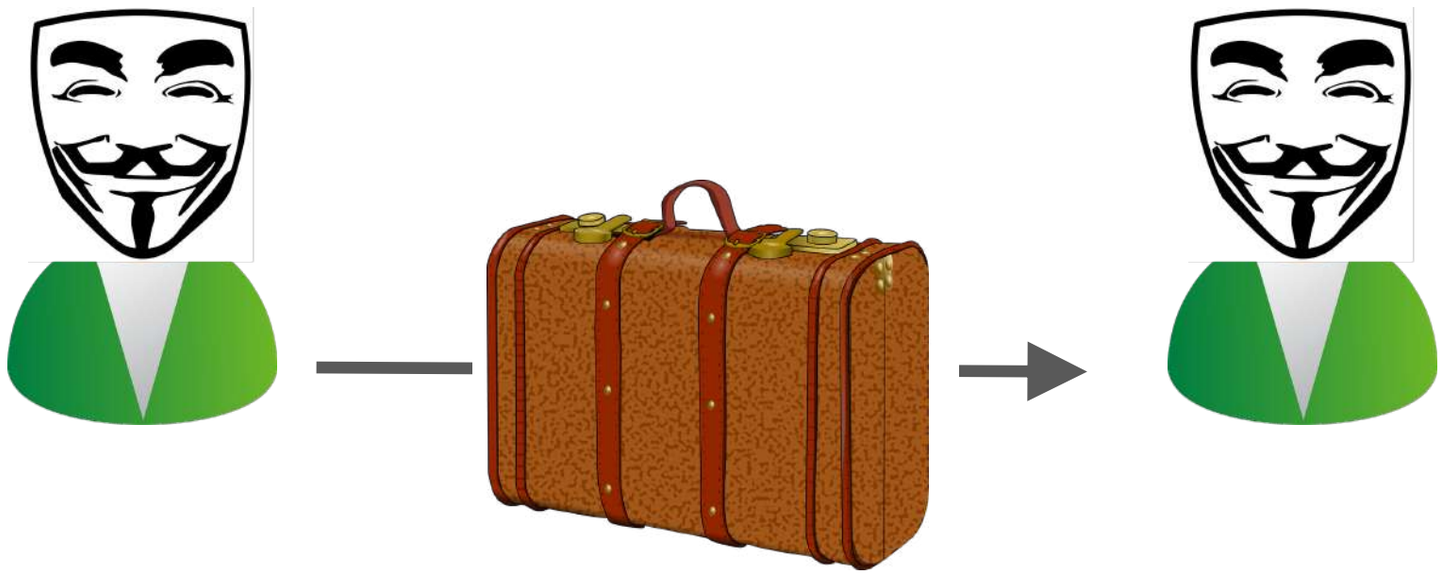
Datenschutz durch Technikgestaltung



- Hashwerte
- Verschlüsselung
- Zero Knowledge Proofs

Zero-Knowledge Proof – Zcash

- Nur Parteien der Transaktion können Details sehen
- Dritte können nur Korrektheit der Transaktion überprüfen
- Privacy by design



Privacy Coins

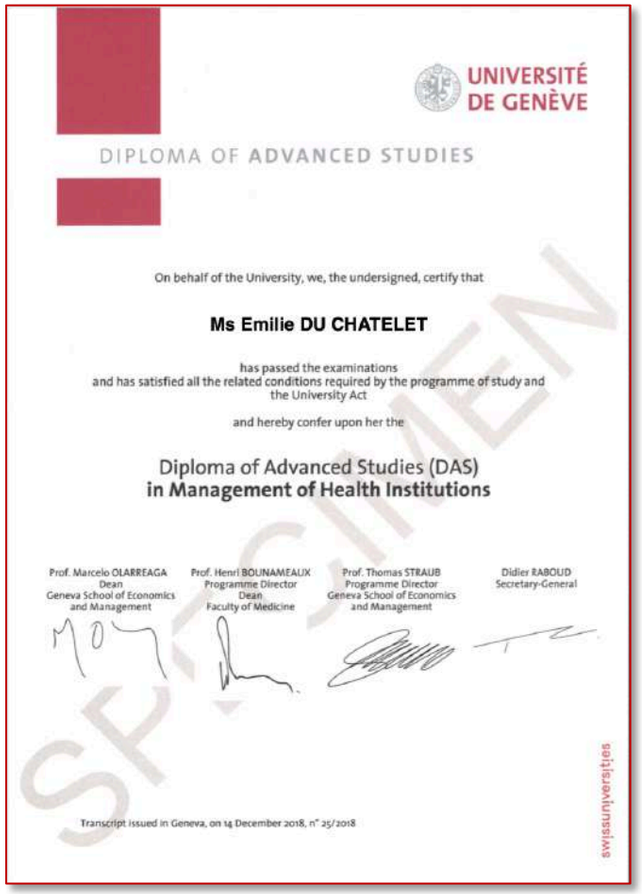
- Transaktionen mit bis zu 5000 CHF
- Ohne Identifizierung
- Ohne KYC

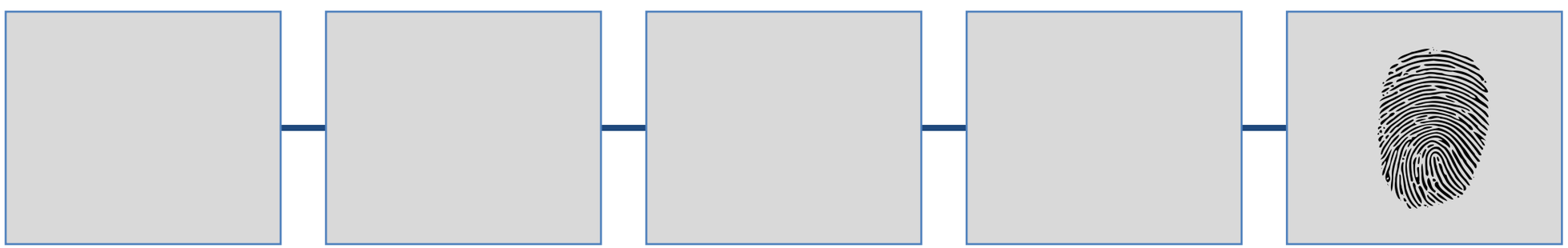
Kryptographische Hashfunktionen

- Digitaler „Fingerabdruck“
- Praktisch eindeutig
- Gleiche Länge (z.B. 43 Zeichen)
- Für digitale Objekte beliebiger Größe
- Kann nicht zurückgerechnet werden

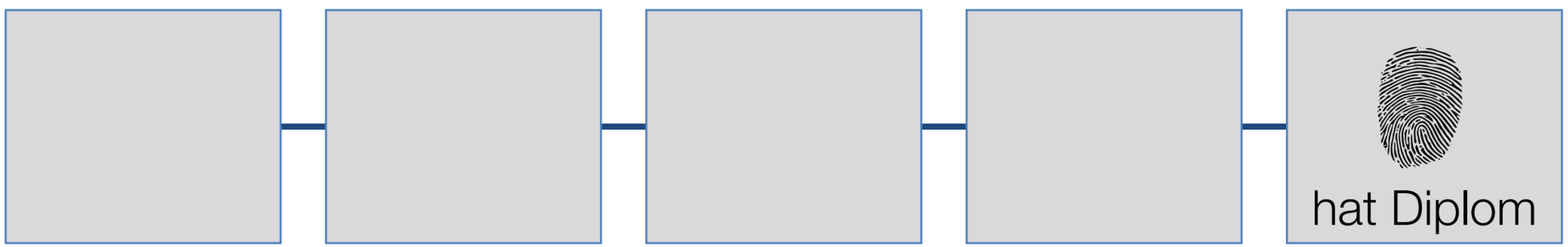
Demo 2

Privatsphäre schützende Nutzung von Hashwerten





Nicht DSGVO-konforme Nutzung von Hashwerten



Sind Hashwerte personenbezogene Daten?

Artikel 29-Gruppe (05/2014, WP216)

Keine der in dieser Stellungnahme beschriebenen Techniken erfüllt zuverlässig die Kriterien einer wirksamen Anonymisierung (d. h. Unmöglichkeit des Herausgreifens einer bestimmten Person, keine Verknüpfbarkeit verschiedener Datensätze zu einer Person und Ausschluss von Inferenzen bezüglich einer Person). Da es jedoch durchaus möglich ist, einige dieser Risiken mit einer bestimmten Technik vollständig oder teilweise auszuschließen, ist eine sorgfältige Planung erforderlich, indem die Anwendung einer

4. Pseudonymisierung

Im Zuge der Pseudonymisierung wird ein Merkmal (in der Regel ein einzigartiges Merkmal) in einem Datensatz durch ein anderes ersetzt. Die natürliche Person kann daher nach wie vor mit großer Wahrscheinlichkeit indirekt identifiziert werden. Dementsprechend kann Pseudonymisierung alleine niemals einen anonymen Datenbestand hervorbringen. Sie wird in dieser Stellungnahme dennoch erörtert, da mit ihrem Einsatz zahlreiche Missverständnisse und Fehler verbunden sind.

Risiken

- **Herausgreifen**
  Mit dem Diplom, finde ich den Hashwert auf der Blockchain. Bei diesem Hashwert finden sich jedoch keine Informationen.

- **Verknüpfbarkeit**
  Jedes Diplome hat einen anderen Hashwert. Eine Verknüpfbarkeit über die Hashwerte ist damit ausgeschlossen.

- **Inferenz**
  Neben dem Hashwert sind keine weiteren Informationen abgelegt und können auch nicht aus dem Kontext abgeleitet werden. Nur mit dem Diplom selbst, kann ich den Hashwert identifizieren, erfahre dann aber nichts Zusätzliches.

Sind Hashwerte personenbezogene Daten?

Art 4 Nr. 1

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Personenbeziehbarkeit?

Erwägungsgrund 26

[3] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. [4] Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

- Nur Mittel, die tatsächlich verfügbar sind.
- Konkretheit der technologische Entwicklungen?
- Rechtliche Wirkung des Erwägungsgrunds?

Wann liegt eine INFORMATION ÜBER eine Person vor?

Matthäus - Kapitel 5

Die Seligpreisungen

1 Da er aber das Volk sah, ging er auf einen Berg und setzte sich; und seine Jünger traten zu ihm, 2 Und er tat seinen Mund auf, lehrte sie und sprach:

3 Selig sind, die da geistlich arm sind; denn das Himmelreich ist ihr. (Psalm 51.19) (Jesaja 57.15)

4 Selig sind, die da Leid tragen; denn sie sollen getröstet werden. (Psalm 126.5) (Offenbarung 7.17)

5 Selig sind die Sanftmütigen; denn sie werden das Erdreich besitzen. (Psalm 37.11) (Matthäus 11.29)

6 Selig sind, die da hungert und dürstet nach der Gerechtigkeit; denn sie sollen satt werden. (Lukas 18.9) (Johannes 6.35)

7 Selig sind die Barmherzigen; denn sie werden Barmherzigkeit erlangen. (Matthäus 25.35) (Jakobus 2.13)

8 Selig sind, die reines Herzens sind; denn sie werden Gott schauen. (Psalm 24.3-5) (Psalm 51.12) (1. Johannes 1.3) (1. Johannes 3.2)

9 Selig sind die Friedfertigen; denn sie werden Gottes Kinder heißen. (Hebräer 12.14)

10 Selig sind, die um Gerechtigkeit willen verfolgt werden; denn das Himmelreich ist ihr. (1. Petrus 3.14)

11 Selig seid ihr, wenn euch die Menschen um meinetwillen schmähen und verfolgen und reden allerlei Übles gegen euch, so sie daran lügen. (Matthäus 10.22) (Apostelgeschichte 5.41) (1. Petrus 4.14) 12 Seid fröhlich und getrost; es wird euch im Himmel wohl belohnt werden. Denn also haben sie verfolgt die Propheten, die vor euch gewesen sind. (Hebräer 11.33) (Jakobus 5.10)

Jörn Erbguth

Vgl. Artikel 29-Gruppe Stellungnahme 4/2007, WP 136

Personenbezogene Daten?

Zu prüfen daher:

Kann
personenbeziehbare Information
aus dem Hashwert und seinem Kontext abgeleitet werden,
die nicht zwingend vorher mitgebracht werden muss?

✓ Hashwert zum Abgleich von e-Mail Adressen

✗ Hashwert wenn gehashte Information sicher gelöscht ist

✗ Hashwert als Zeitstempel, ohne Zusatzinfo oder Kontext

Wer ist Verantwortlicher i.S.d. DSGVO?

Infrastruktur

- Public Blockchain
- Permissioned Blockchain

Smart Contract

- Nur bereitgestellter Code
- Möglichkeit Updates einzuspielen

Transaktion

- Autorisierung mit privatem Key
- Dapp oder Dienstleister

Pflichten der Verantwortlichen und Auftragsverarbeiter

- Verantwortliche müssen sich identifizieren
- Auftragsverarbeitungsvereinbarungen
- Verantwortliche müssen Auftragsverarbeiter kontrollieren

Haushaltsausnahme für privat motivierte Transaktionen?

- CNIL sieht Haushaltsausnahme z.B. für privat motivierte Bitcoin-Transaktionen
- Transaktionen öffentlich (EuGH Lindqvist?)
- Ohne Haushaltsausnahme hätten Privatleute Pflicht zur Identifizierung!
- Kann DSGVO Verbot der privaten pseudonymen Nutzung z.B. von Bitcoin begründen?

Rechtfertigung (Art. 6 Abs. 1 DSGVO)

- Einwilligung ⚡ Widerruf (Art. 7 Abs. 3)
- Berechtigtes Interesse ⚡ Widerspruch (Art. 21 Abs. 1)
- Vertrag
- Rechtliche Verpflichtung

Fazit

Datenschutzkonformer Einsatz von Blockchains ist möglich

a) Keine personenbezogene Daten auf der Blockchain

b) Datenschutz durch Technikgestaltung

c) Permanente Rechtfertigung für Ablage auf der Blockchain

d) Transaktion wird durch Betroffenen vorgenommen

e) Blockchains, die „vergessen“ können

Viele potentielle Einsatzbereiche sind aber ausgeschlossen!

Privacy by Design und ggf. DSFA (DPIA) erforderlich.

Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Diskussion