DSGVO-konformer Einsatz von Blockchains

Swiss Legal Tech Conference, Zürich, 18.9.2018

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

joern@erbguth.ch +41 787256027

Datenschutz vs. Blockchain

Datenschutz

Blockchain

Recht auf …

Art. 16: Berichtigung

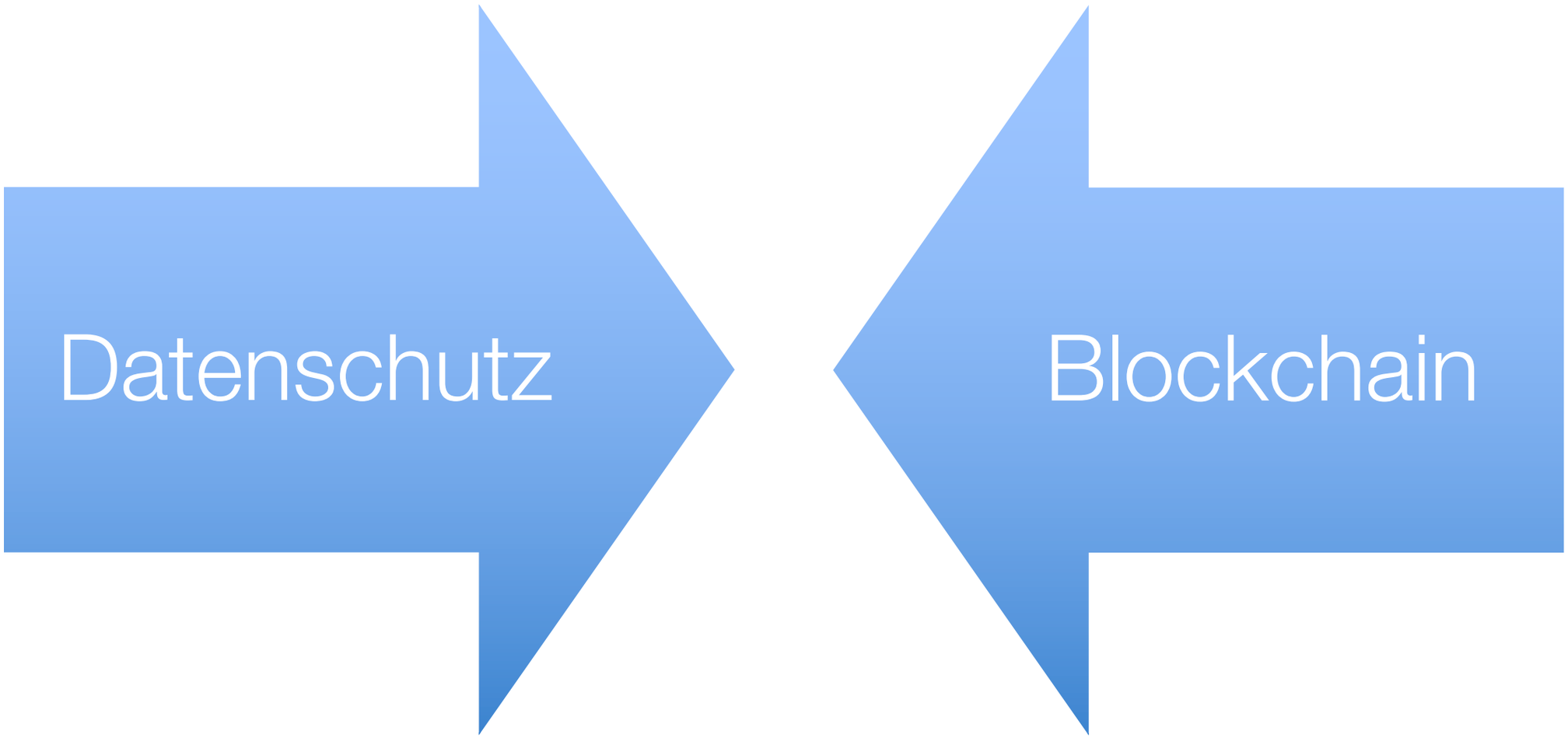
Art. 17: Löschen

Art. 18: Einschränkung der Verarbeitung

Unveränderlich

Öffentlich

Datenschutz vs. Blockchain



Klare Verantwortlichkeiten
Verantwortlicher (Controller)
Auftragsverarbeiter (Processor)

Verteilte Verantwortung
Anonyme Teilnehmer

Personenbezogene bzw. personenbeziehbare Daten?

Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Nr. 1 DSGVO)

Erwägungsgrund 26

- Einer **Pseudonymisierung** unterzogene personenbezogene Daten, die durch **Heranziehung zusätzlicher Informationen** einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.

- 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.

- Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder **personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann**.

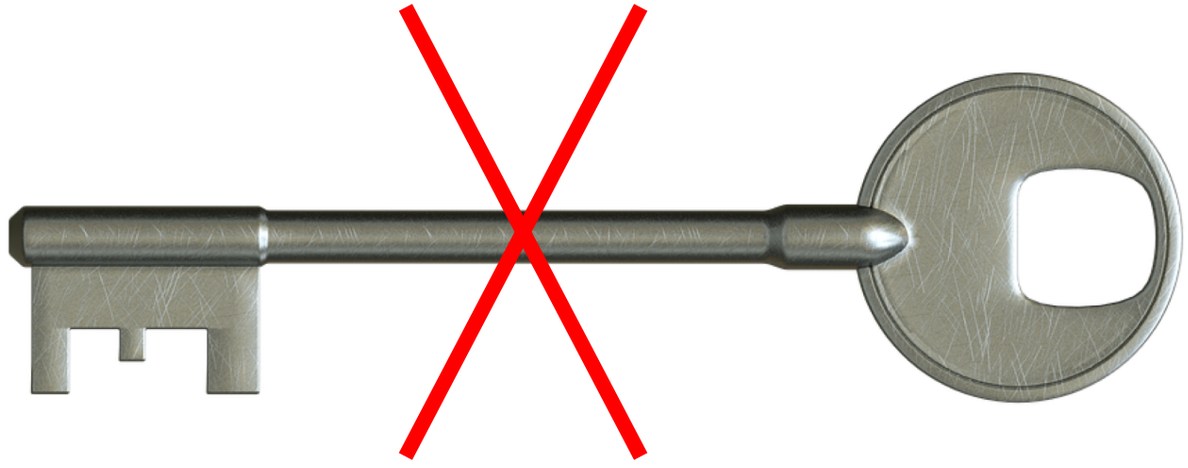
Personenbeziehbare Daten - Beispiele

- ✓ IP-Adressen
- ✓ Bitcoin-Adressen
- ✓ ”Anonymisierte” Bewegungsprofile
- ✓ “Anonymisierte” Browserhistorie
- ✗ Aggregierte Bewegungsprofile
- ✗ Aggregierte Browserhistorie

Achtung: Falsche Pauschalisierungen!

Verschlüsselung

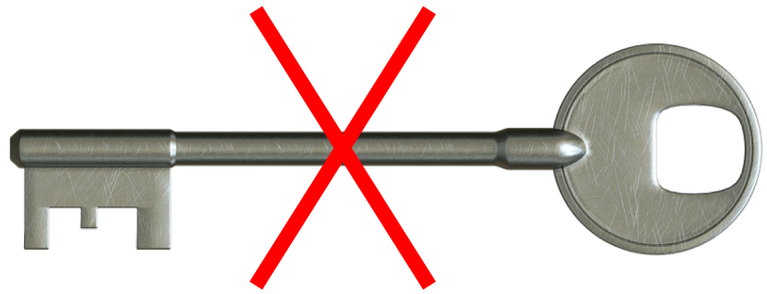
Löschen des Schlüssels = Löschen der Daten




SAMSUNG
MMCQE28GFMUP – MVA
DFK3O0A842 – 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.
SERIAL ATA
MIC
2. 인 증 번 호 : SEC – M – SLIM28GUSATA(B)
4. 제 조 년 월 일 : 2008.10.07
FC SAMSUNG MMCQE28GFMUP – MVA
SAMSUNG 837 K9HCG28U1M PCK0

DSGVO konforme Löschung?

- Löschen des Schlüssels = Löschen der Daten?



- Existiert noch eine Schlüsselkopie?
- Wird das Verschlüsselungsverfahren irgendwann unsicher?

Einsatzbereich Verschlüsselung

- Kontrollinstanzen
- Kontrollrecht ggf. zeitlich begrenzt
- Vertragspartner
- Betroffene selbst
- Selektives Löschen in unveränderbaren Datenbeständen

Hashwert als bessere Alternative zur Verschlüsselung

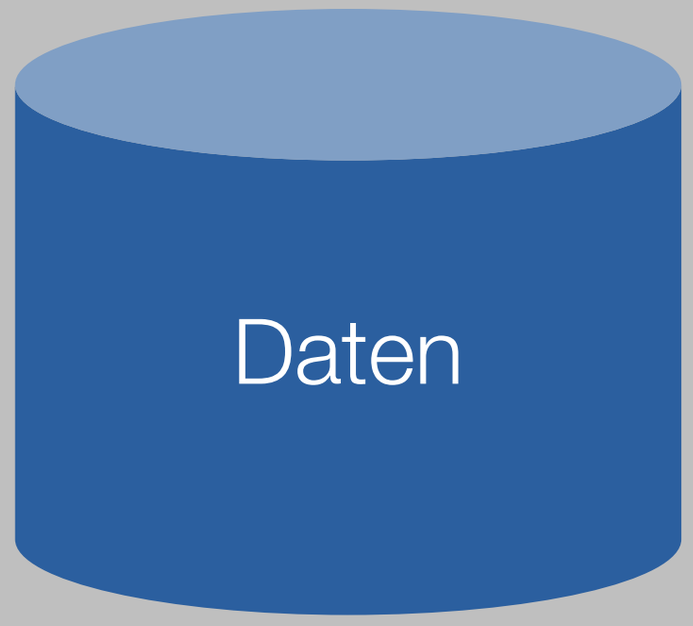
Öffentlich

Geheim

Hashwert als bessere Alternative zur Verschlüsselung

Öffentlich

Geheim



Kryptographische Hashfunktionen

- Dienen als digitale Fingerabdrücke
- Praktisch eindeutig
- Konstante Länge (z.B. 32 Bytes)
- Für digitale Objekte beliebiger Größe
- Aus einem Hashwert kann (praktisch) kein passendes Objekt errechnet werden

Demo 2

Beispiele für Hashwerte

- Switzerland

  `2275583196D791405892AACA0D87743C872F3FC0CF3308A6C3EF82528918AA8A`

- Switzerland.

  `43CF6F3ECA7253FFAB1FD5104172280189B91FDD5FA26774FCA6475FFA1E2EC9`

- 

  `8C4B4C4E211BA8C1A62DE2A3A6CA5AC8BFF501C14410100DD90D5077A0AC061E`

Hashwerte zur Generierung von Zeitstempeln

Hash: F4D38DFFE4304CB887587E3FC6B15717328E23471BECD259F58E0F3CB63722D2

Kryptografische Hashwerte, datenschutzkonform

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

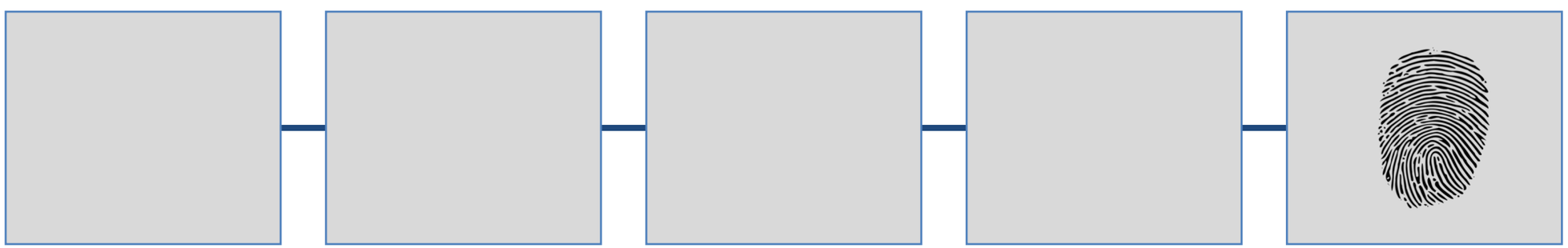
Diplom-Jurist Univ.

(Dipl.-Jur. Univ.)

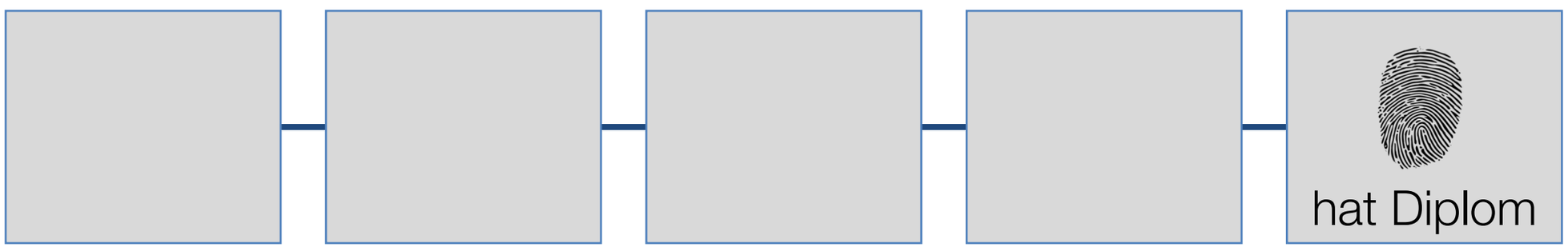
aufgrund der gemäß Ausbildungs- und Prüfungsordnung für Juristen (JAPO) in der jeweils gültigen Fassung am 23. Juli 1992 bestandenen Ersten Juristischen Prüfung.

Passau, den 24. Januar 2018

(Prof. Dr. Hans-Georg Dederer)
Dekan



Kryptografische Hashwerte, nicht datenschutzkonform



Einsatzbereiche kryptografische Hashwerte

- Externe Dokumente validieren
- Zeitstempel
- Proof of Existence
- Basisfunktionalität für Kryptographie und DLT

Auch Hashwerte bergen ein Personalisierungsrisiko!

Zero Knowledge Proof

Beweis etwas zu wissen,
ohne das Wissen zu offenbaren

Einfacher Zero Knowledge Proof

Öffentlicher Schlüssel

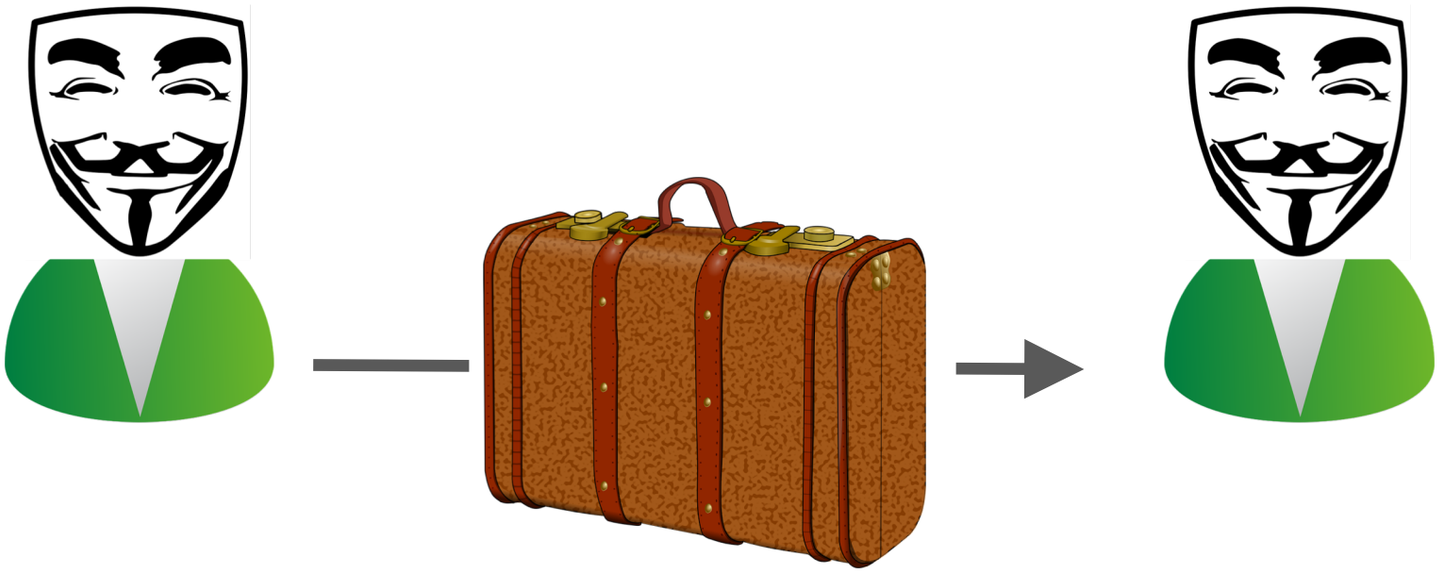
Privater Schlüssel

Zero Knowledge Proof – klassisches Beispiel

farbensehend

Zero Knowledge Proof

- Technische “Zweckbindung” von Daten
- Nur Korrektheit der Transaktion nachweisbar



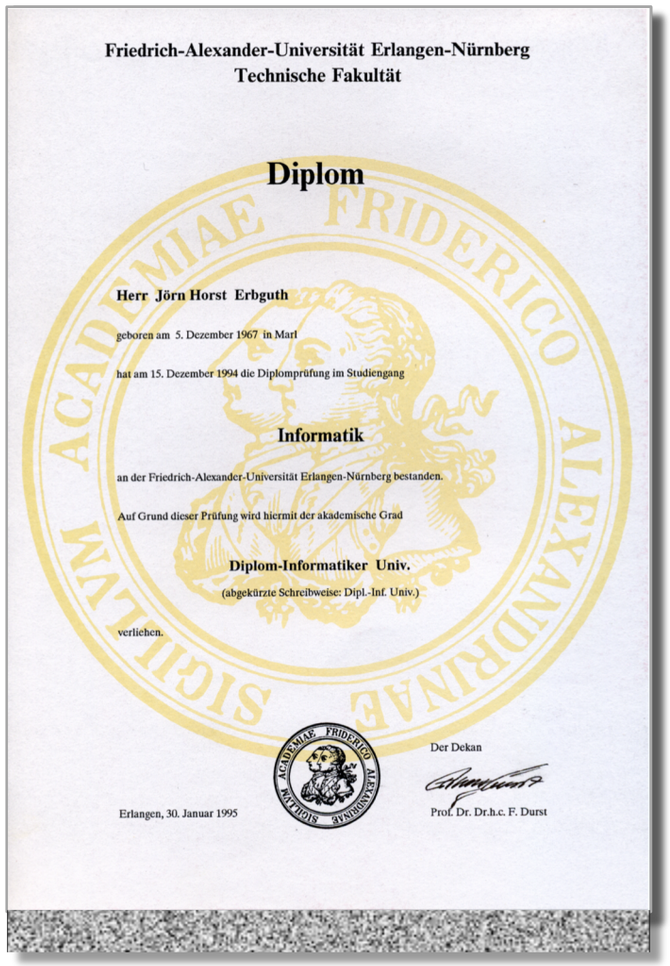
Vorteile

- Zugriffsschutz wirkt auch gegen Administratoren
- Zugriffsmöglichkeiten nachträglich nicht veränderbar
- Schutz vor Hackern, die Firewalls überwinden
- Schutz der Daten vor Manipulation

Unveränderliche Daten auf der Blockchain - Risiken

- Überbordende Auslegung des Personenbezugs durch die Aufsichtsbehörden
- Isolierte Betrachtung der Daten nicht ausreichend
- Personenbezug kann sich nachträglich durch äussere, nicht kontrollierbare Ereignisse ergeben
- Daten auf der Blockchain bleiben dennoch bestehen
- Haftung für die Veröffentlichung von einst anonymen aber später personalisierbaren Daten unklar

Chamäleon Hashfunktion



Friedrich-Alexander-Universität Erlangen-Nürnberg
Technische Fakultät

Diplom

Herr Jörn Horst Erbguth

geboren am 5. Dezember 1967 in Marl

hat am 15. Dezember 1994 die Diplomprüfung im Studiengang

Informatik

an der Friedrich-Alexander-Universität Erlangen-Nürnberg bestanden.

Auf Grund dieser Prüfung wird hiermit der akademische Grad

Diplom-Informatiker Univ.

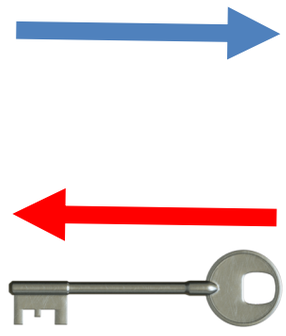
(abgekürzte Schreibweise: Dipl.-Inf. Univ.)

verliehen.

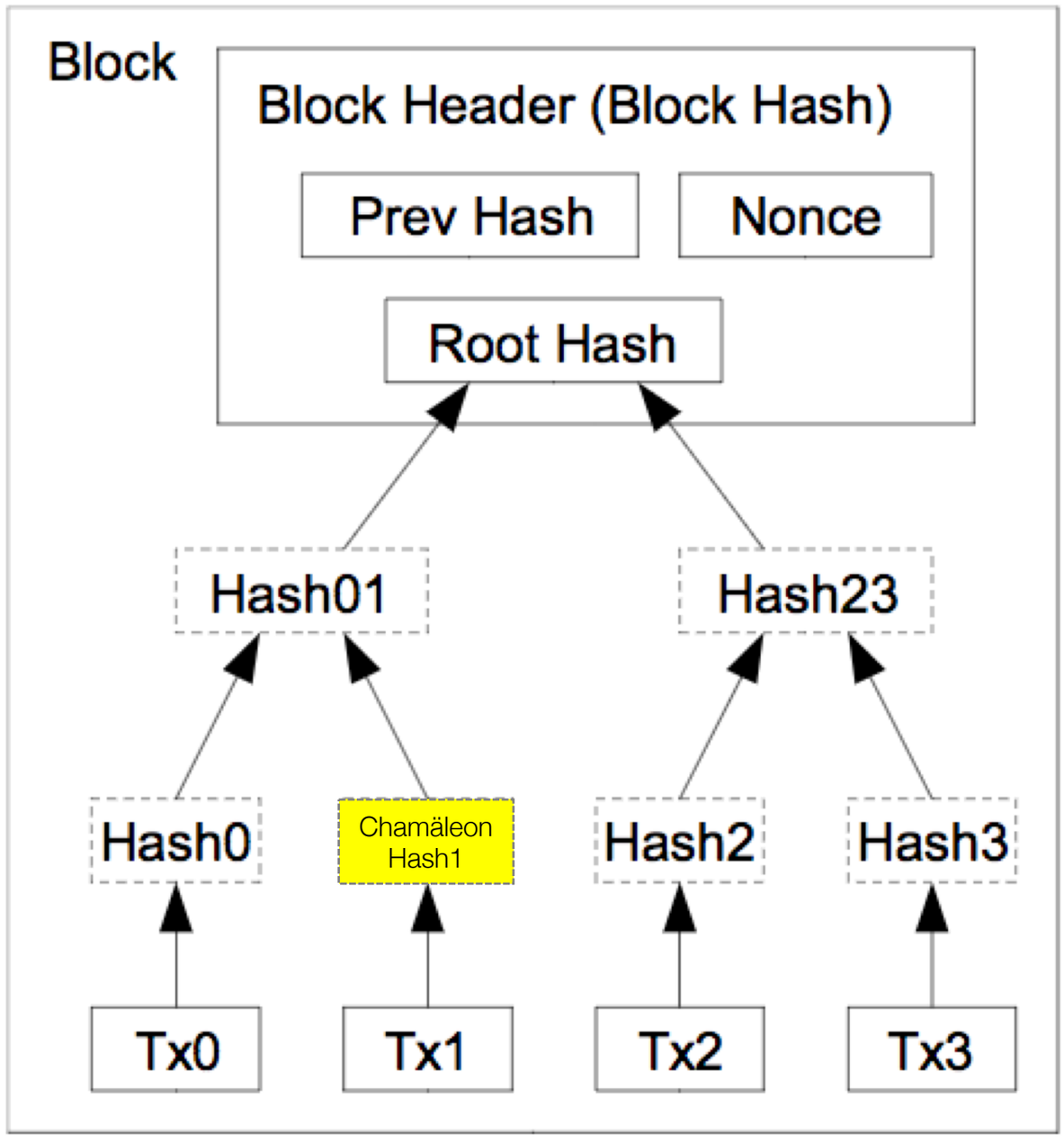
Erlangen, 30. Januar 1995

Der Dekan

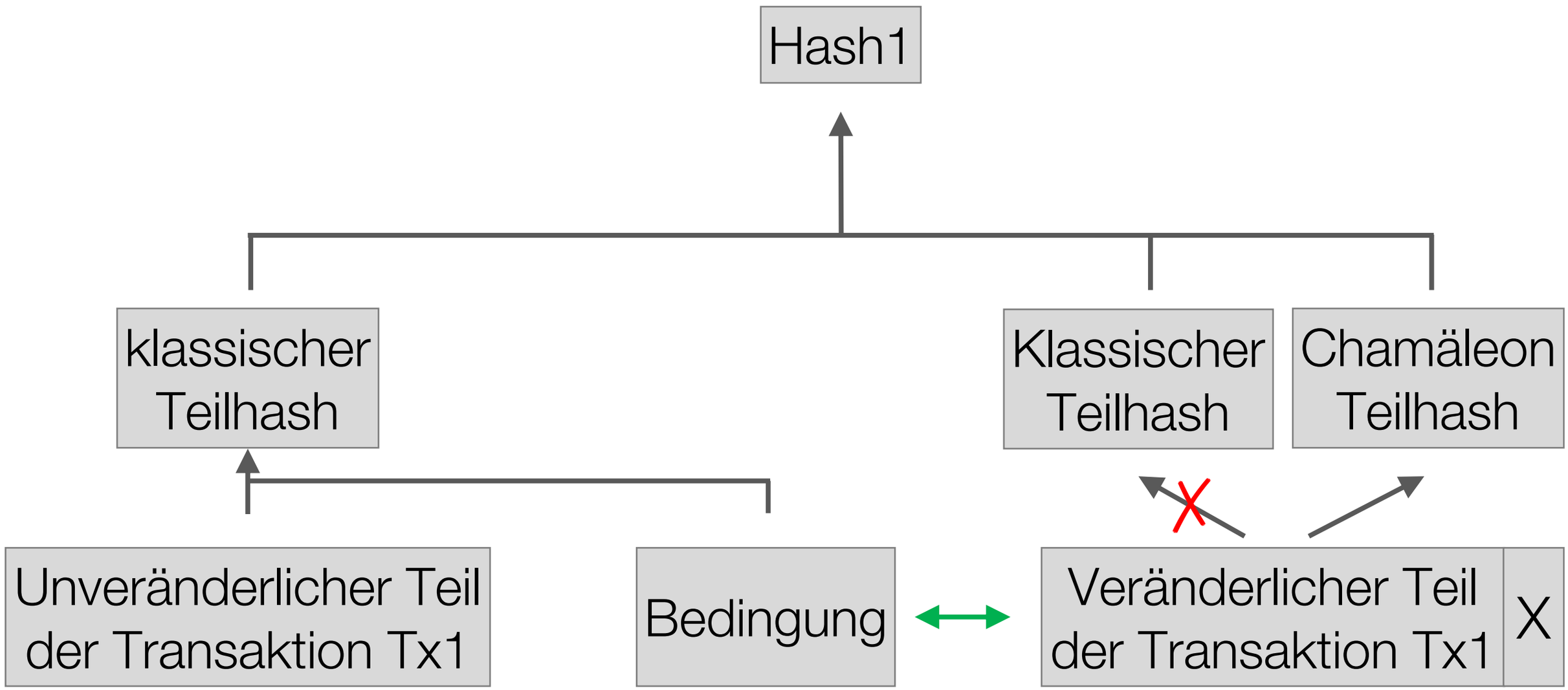
Prof. Dr. Dr.h.c. F. Durst



Chamäleon Hashfunktionen



Chamäleon Hashfunktionen



Einsatzbereich Chamäleon-Hashes

- Varianten öffentlicher Blockchains bei denen ein vorab spezifizierter Teil unter bestimmten Bedingungen modifiziert werden kann.

- Transaktionen,
  - bei denen **bestimmte Details**
  - z.B. nach **Firstablauf**
  - unter bestimmten **Bedingungen**
  - von **autorisierter Stelle**

  geändert werden dürfen

Rechtmäßigkeit der Verarbeitung (Art. 6)

- Einwilligung (Abs. 1 a)
- Erfüllung eines Vertrags mit der betroffenen Person (Abs. 1 b)
- Erfüllung einer rechtlichen Verpflichtung (Abs. 1 c)
- Berechtigte Interessen (Abs. 1 f)

Verarbeitung auf Grund einer Einwilligung

- Anforderungen an die Einwilligung

  Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. (Erwägungsgrund 32)

- Widerrufbarkeit der Einwilligung (Art. 7 Abs. 3)

Schlechteste Form der Rechtfertigung!

Erfüllung eines Vertrages mit dem Betroffenen

- Muss für die Vertragserfüllung erforderlich sein
- Vertrag muss nicht mit dem Verarbeiter bestehen
- Kann nicht widerrufen werden
- Z.B. Bezahlung mit Bitcoins

Erfüllung einer rechtlichen Verpflichtung

- Personenbezogene Daten müssen auf Grund einer rechtlichen Verpflichtung mit gespeichert werden

- Z.B. KYC, AML

Aber: Rechtliche Verpflichtung sieht meistens keine zeitlich unbegrenzte Speicherpflicht vor

Berechtigte Interessen

- Löschen würde Blockchain zerstören

- Erwägenswert, wenn das Medium Blockchain auf Grund der Vorgabe des Betroffenen gewählt worden ist.

Wer ist eigentlich ”Verantwortlicher”?

- Knotenbetreiber?
- der Mineur, der den Block mined und verteilt?
- alle Mineure zusammen?
- Der Anwender, der eine Transaktion signiert und an die Blockchain sendet?
- Die Exchange oder der Wallet Service, die die Transaktion für den Anwender signieren und an die Blockchain senden?

Wer ist eigentlich ”Verantwortlicher”?

Art. 4 Nr. 7 DSGVO

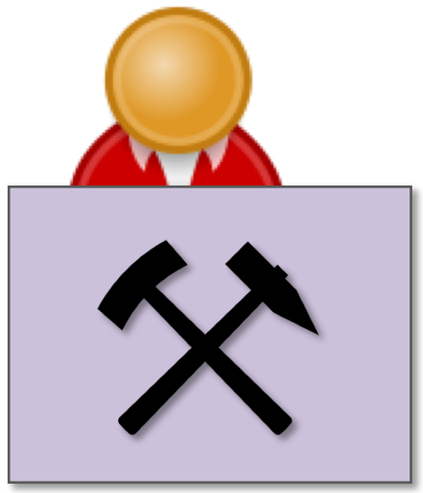
„Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die **allein** oder **gemeinsam** mit anderen über die **Zwecke und Mittel** der Verarbeitung von personenbezogenen Daten entscheidet

Art. 26 DSGVO

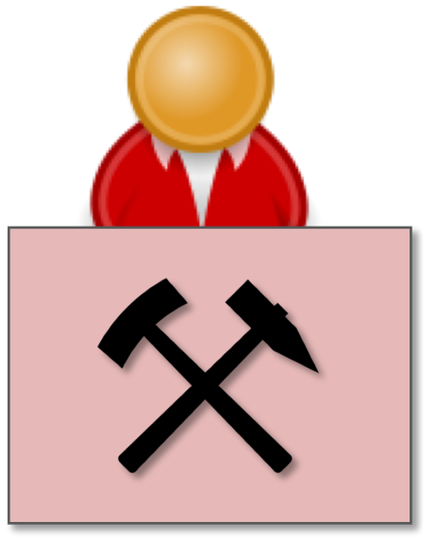
Legen zwei oder mehr Verantwortliche **gemeinsam** die **Zwecke** der und die **Mittel** zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche**

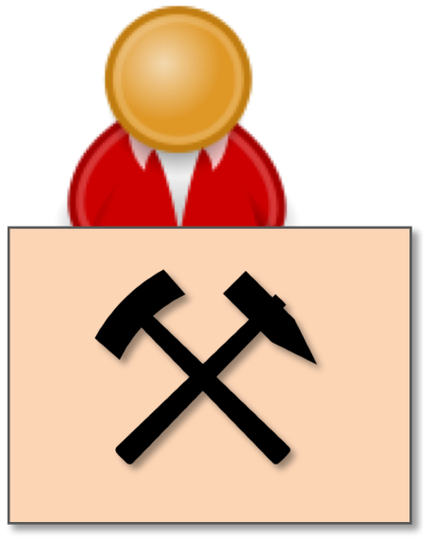
In der englischen Fassung „**controller**“

Mining



Transaktion Tra
nsaktion Transa
ktion Tr
n Trans



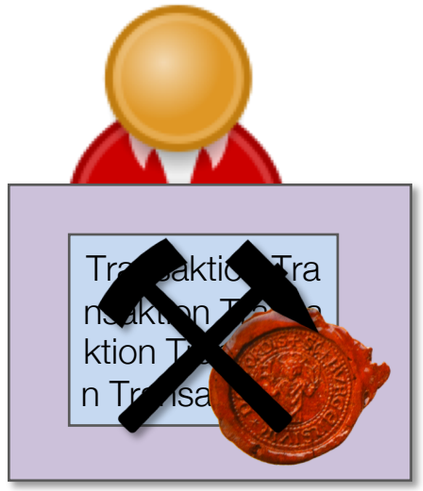


Ablehnen einer Transaktion durch Miner

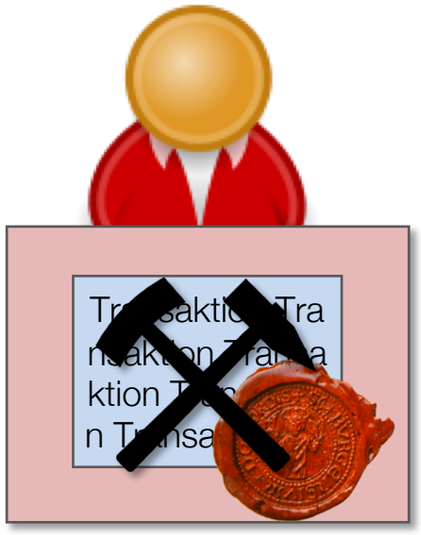
- Jeder Miner selektiert Transaktionen
- Selektion nur von Bedeutung, wenn Miner als erstes passende Nonce findet
- Transaktion kann aber Teil eines Folgeblocks werden

Eine Transaktion wird nur verhindert, wenn alle Miner sie ablehnen

Ablehnen eines Blocks

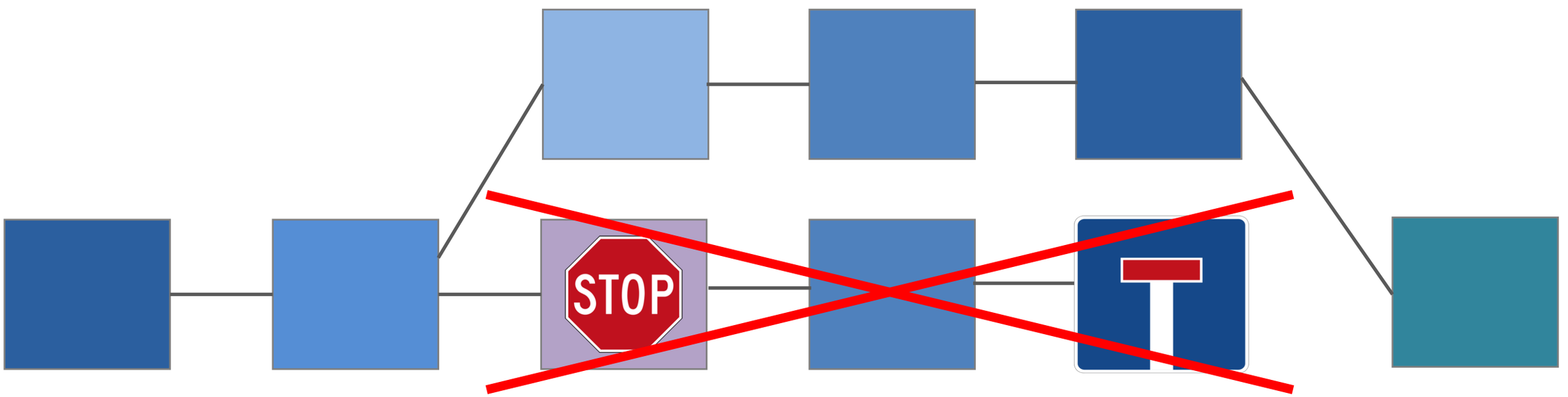


Transaktion Tra
nsaktion Transa
ktion Tr
n Trans



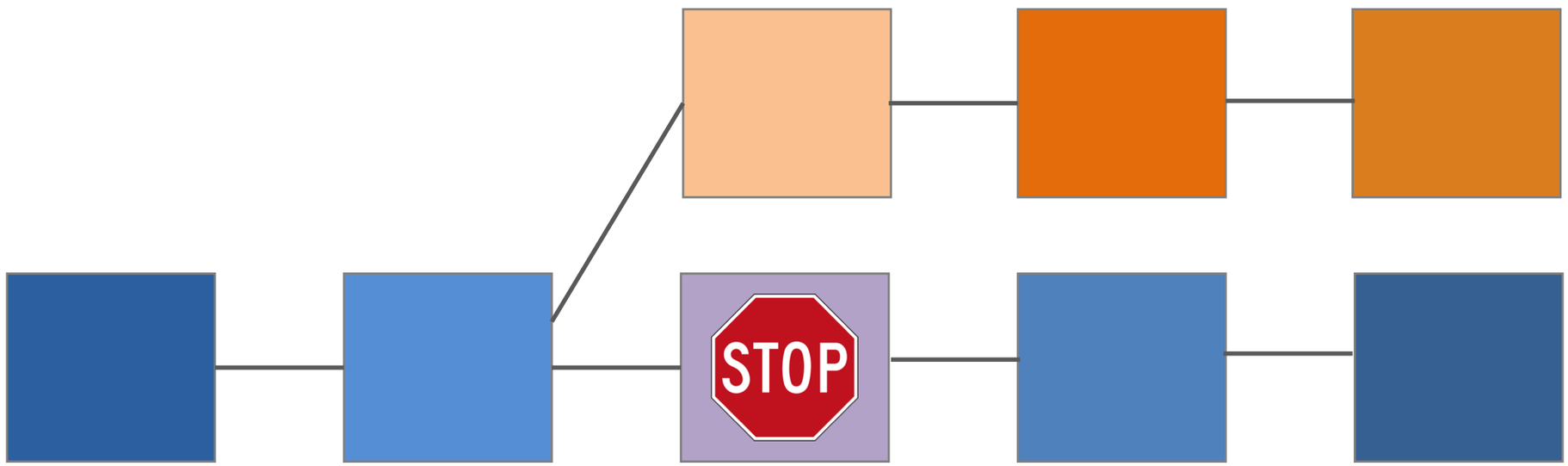
Ablehnen eines Blocks durch Miners

- Miners können einzelne Blöcke ablehnen
- Ablehnung nur wirksam wenn Ablehnung von mindestens 50% der Rechenleistung geteilt wird



Hard Fork

- Regeln der Blockchain werden geändert
- Neue und alte Software inkompatibel
- Ergebnis: Zwei unterschiedliche Blockchains
- Unabhängig davon wie viele Miner mitmachen
- Knotenbetreiber, Exchanges etc. entscheiden, welche Blockchain(s) danach akzeptiert werden



Sind Knotenbetreiber Auftragsverarbeiter?

Art. 28, 29 DSGVO

- Vertrag mit Verantwortlichem (Schriftform auch elektronisch)
- Weisungsgebunden
- Kontrolle

Vertrag und Kontrolle über die Blockchain-Software?

Verantwortlicher bei Permissioned Blockchains

- Zentrale Stelle koordiniert und gibt Bewilligung?
- Teilnehmer sind bekannt und koordinieren sich
- Löschungen prinzipiell einfacher durchführbar

Wenn aber zentrale Stelle Löschung nach Belieben anordnen kann, welchen Mehrwert bietet diese Blockchain noch?

Governance

Blockchain schafft Vertrauen durch Dezentralisierung

Governance muss dezentral erfolgen

Rechtssystem muss Regelungen für dezentrale Governance schaffen

Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Diskussion