Revolution Blockchain? Realistische Einsatzmöglichkeiten aus Sicht des Datenschutzes

Benjamin Walczak

Sommerakademie 2018
„Update nötig: Beschäftigtendatenschutz im digitalen Zeitalter 4.0“
10.09.2018, Kiel

Überblick

1. Einführung in Blockchains
   - Geschichte
   - Begriffe und Funktionsweisen
   - Charakteristika und Risiken
2. Anwendungsbeispiele
   - Katasterwesen in Schweden
   - Zug ID
3. Blockchains und Datenschutz

Einführung in Blockchains: Geschichte

1990er erste Grundlagen (kryptografische Verkettung, ...)

2008 „Satoshi Nakamoto“ stellt Bitcoin White Paper vor

2014	Bitcoin-Blockchain:	20 GB
2015		30 GB
2016		50 GB
2017		100 GB

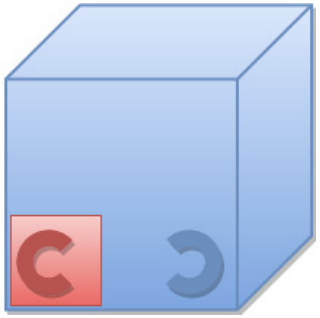
2014 Blockchain 2.0 (Smart contracts, Ethereum)

2016 Großteil der Tech-Unternehmen startet eigene Blockchain-Projekte

Blockchain: Die Begriffe

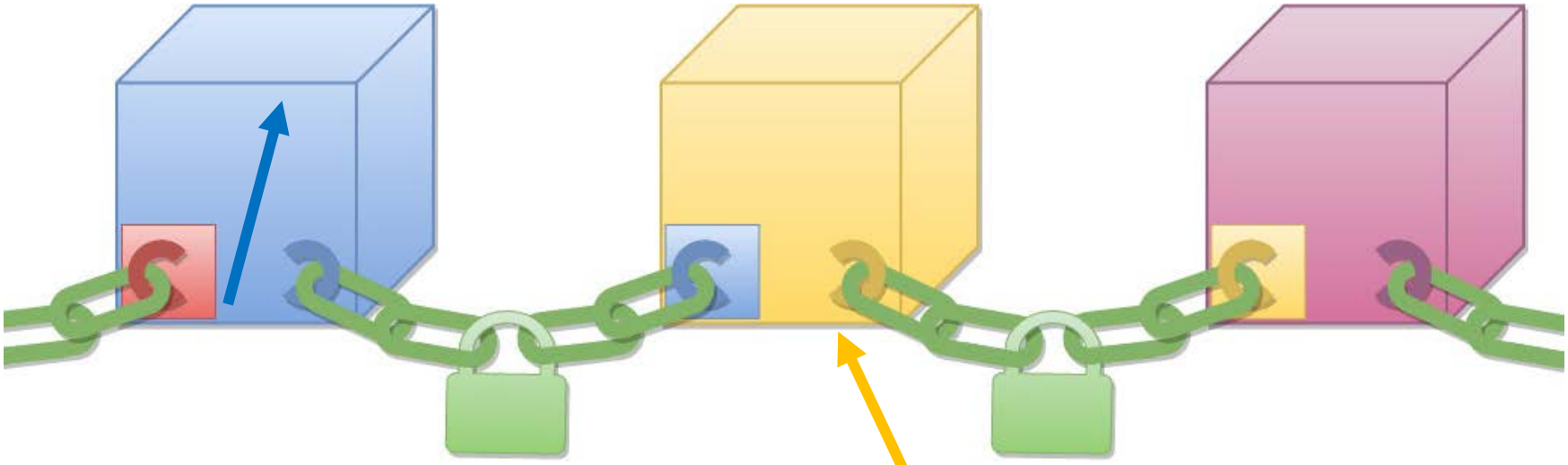
- **Hashfunktion**
  - kryptografische Funktion: Eingabe → Hashwert
  - Aus Hashwert kann nicht die Eingabe ermittelt werden!

- **Block**
  - Sammlung von Dateneinträgen (Transaktionen o.ä.)
  - mit Zeitstempel
  - mit Hashwerten
    - des kompletten vorangehenden Blocks
    - des Blocks selbst



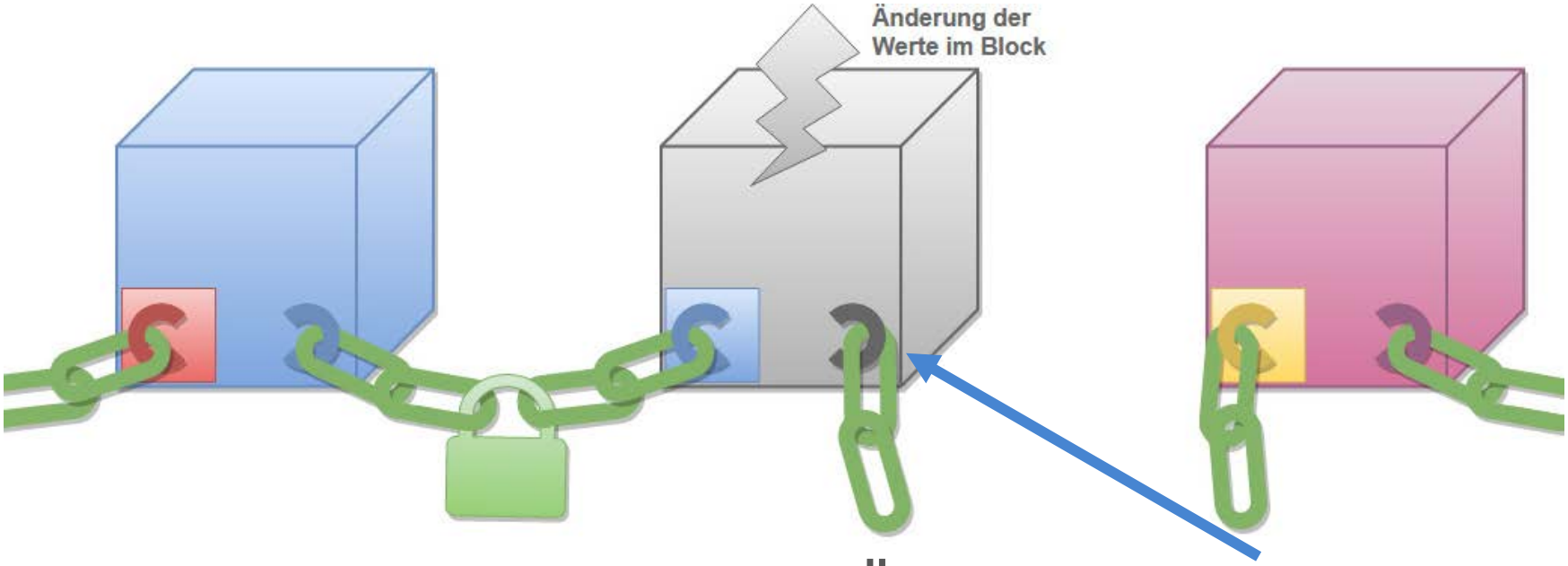
- **Konsensfindung**
  - Ergänzung neuer Blöcke
  - Missbrauchsverhinderung, z.B. durch hohen Aufwand

Funktionsweise einer Blockchain: kryptografische Verkettung



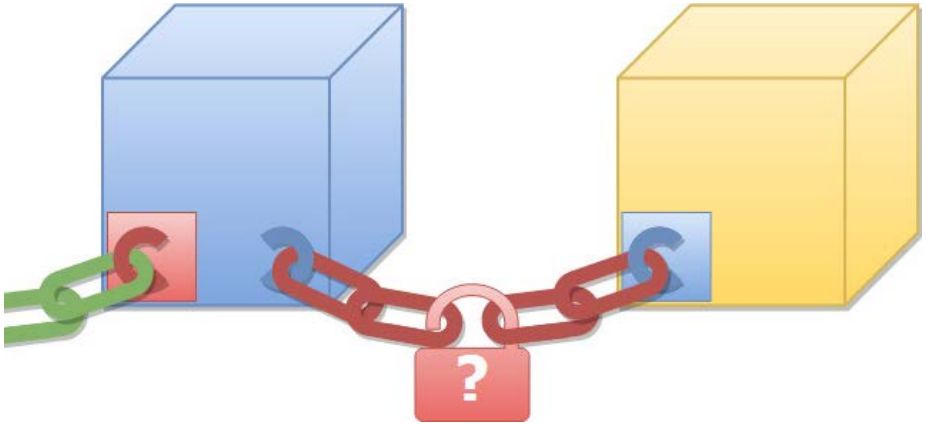
- **Hashwert** eines Blocks wird im **nächsten Block** gespeichert und dadurch Bestandteil des nächsten Blocks.
- Bereits eine geringfügige Änderung eines Blocks würde seinen Hashwert verändern.

Funktionsweise einer Blockchain: kryptografische Verkettung



- Im mittleren Block gab es eine **Änderung**, der **Hashwert** hat sich auch geändert.
- Die Kette ist unterbrochen, da der nächste Block nun den falschen Hashwert enthält. Wird dieser geändert, ändert sich auch dessen Hashwert usw.

Funktionsweise einer Blockchain: Konsensfindung



- Wer darf einen neuen Block erstellen?
- Verschiedene Auswahlverfahren:
  - Proof of Work (Mining)
  - Proof of Stake
  - ...
- Akzeptanz des Verfahrens bei allen Beteiligten notwendig

Funktionsweise einer Blockchain: Verteilte Buchführung

- Dezentrales Speichern bei gleichberechtigten Mitgliedern
- Viele Kopien weltweit, die durch Konsensverfahren identisch bleiben
- Prinzipiell muss immer die ganze Kette gespeichert werden, um Integrität sicherzustellen

Spezifikationen

- Offenheit
  - Permissionless
  - Permissioned
- Block-Größe
- Block-Zeit
- Konsensfindung (s.o.)

- Public
- Private

Charakteristika

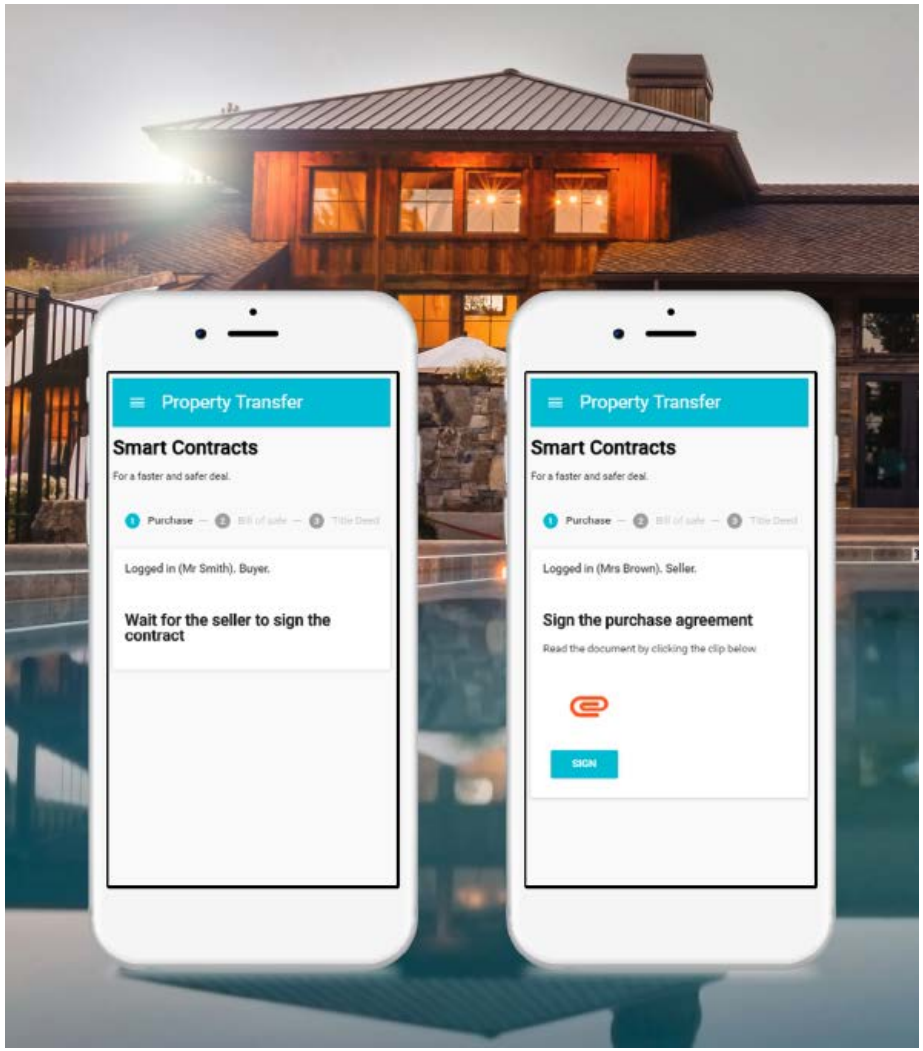
- Daten:
  - grundsätzlich „Registerdaten“, die nicht häufig geändert werden müssen
  - Daten, die nicht gelöscht werden müssen
- Anreiz für Speichern und Verifizieren von Blöcken, z.B.
  - Auftrag
  - Belohnung bei Block-Erstellung (Mining)
- Software-Änderungen sehr aufwendig (Soft/Hard Forks)

Risiken der Technologie

- Sicherheitslücken in der Software
  (2011 Mt. Gox-Lücke, 2016 DAO-Hack)

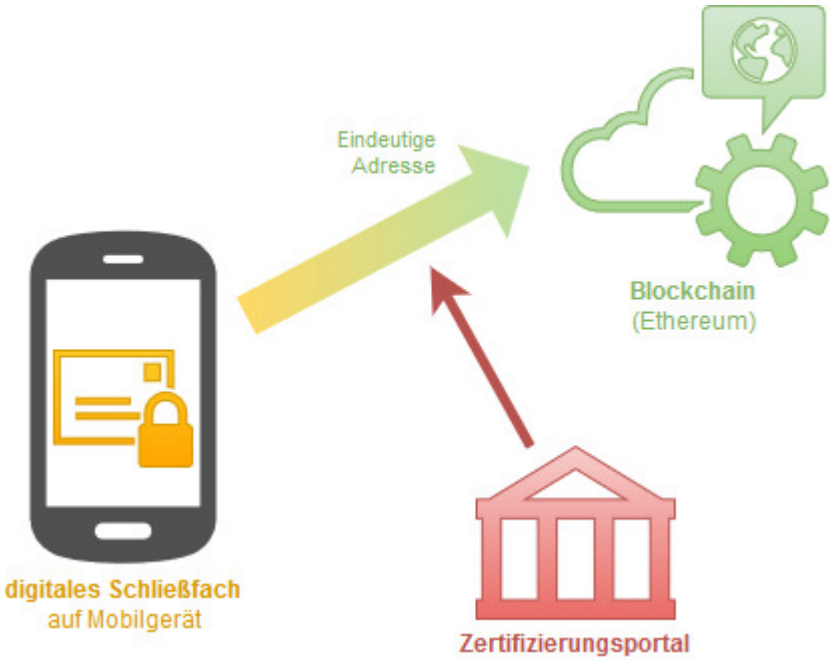
- Manipulation der Konsensfindung
  - 51%-Angriff
    Mehrheit der Miner manipuliert neue Blöcke
  - Konsensverfahren bevorteilt einzelne

Beispiel: Katasterwesen in Schweden

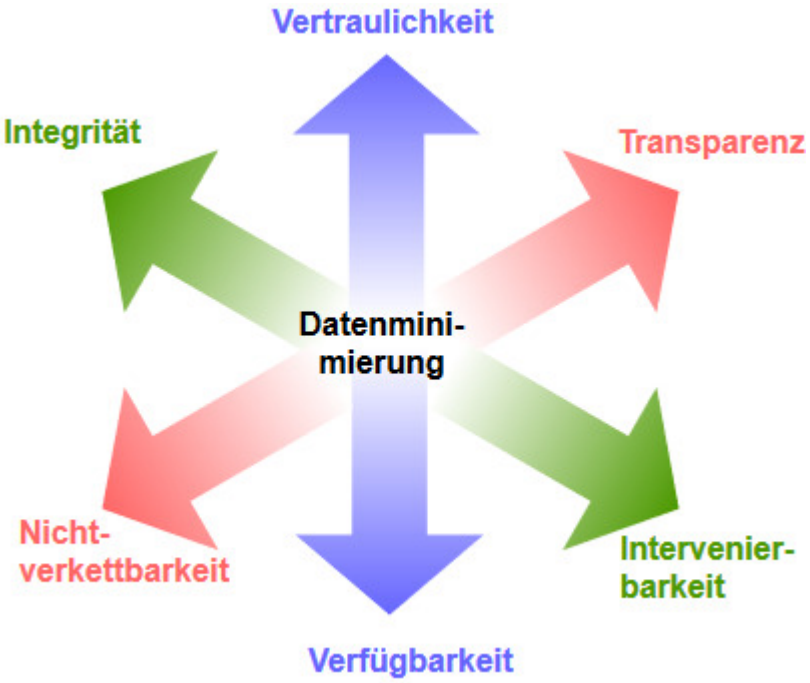


Beispiel: Zug-ID

- Seit 2016 Bitcoin als Zahlungsmittel
- Seit 2017 digitale Identität eingeführt
- Personenbezogene Daten liegen gesichert auf dem Mobilgerät
- In der Blockchain gibt es eine eindeutige Adresse, zertifiziert vom Einwohner-meldeamt

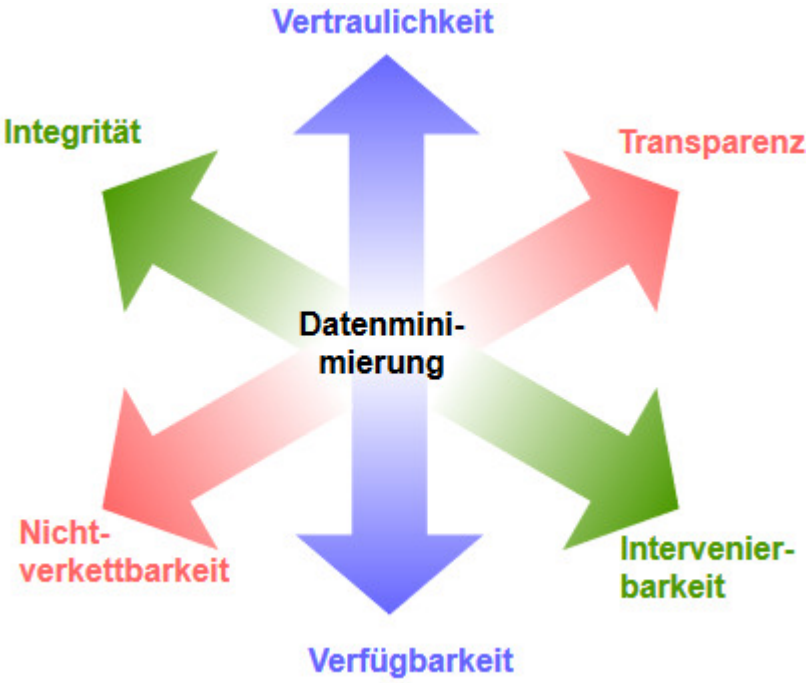


Blockchains und Datenschutz



- Blockchains bieten große Vorteile hinsichtlich Verfügbarkeit, Transparenz und Integrität.
- Blockchain-basierte Währungen werden oft für anonyme Zahlungen verwendet.
- Eine zentrale Überwachung ist sehr schwer.

Blockchains und Datenschutz



- Blockchains bieten wenig für die Gewährleistungsziele Vertraulichkeit, Nichtverkettbarkeit und Intervenierbarkeit.
- Grundsatz Datenminimierung ist durch dauerhaftes Speichern auch nicht erfüllt.
- Datenschutzrecht kaum anwendbar; berechtigte Interessen nicht durchsetzbar

Vielen Dank