Blockchain: Details & mögliche Usecases

Beta 0.1 ;-)

AUSTRIAPRO
Dr. Christian Baumann

21.9.2016

Inhalt

- Konzept von Blockchains
- Usecases
  - Bereiche
  - Beispiele
- Typisierung
- Next Steps
  - Mitarbeit bei TeleTrusT.de – AG Blockchain
    - „Bundesverband IT-Sicherheit e.V.“
  - Geplante Veranstaltung

Blockchain - Konzept

- Konzept
  - Verteilte, fälschungssichere Datenstrukturen
  - Daten in Transaktionen
    - (zeitlich) protokolliert
    - Nachvollziehbar
  - Transaktionen bilden „Blöcke“
    - Plus Metainformationen
  - Blöcke sind kryptografisch „verkettet“
  - => „Block-Kette“

Blockchain - Analogie

- Analogie
  - „Distributed Ledger“ => „verteiltes Hauptbuch“
  - Hauptbuch: z.B. Wirtschaftsprüfer bestätigen Korrektheit der Informationen
  - Blockchain: kryptografische Verfahren (Hashverfahren und digitale Signaturen) stellen die Korrektheit der Transaktionen und zeitliche Abfolge sicher
  - „Verteilt“ – Peer-to-Peer
    - Keine zentrale Speicherung
    - Nicht (kaum) „zerstörbar“ (zensierbar …)

Usecases – Bereiche 1/2

- Kryptowährungen
  - „Zukunft des Geldes?“
    - Bitcoin: nur erste Implementierung (!)
- Fintech
  - (Erforschung von) neuen Finanzlösungen
  - „R3-Blockchain Konsortium“ (50 Banken/Versicherungen)
  - 20 Mia USD/Jahr weniger Abwicklungskosten
- Smart Contracts
  - Automatisierte Abwicklung von Verträgen
    - Z.B. Automatisierung der Prüfung der Vertragserfüllung

Usecases – Bereiche 2/2

- Identity & Access Management
- Ownership „real“
  - „Zuordnung Dinge zu Identitäten“
  - Immobilien, Grundbesitz … Diamanten
- Ownership „virtuell“
  - „Copyright“ Musikindustrie, Kunst …
- Notarization
  - Bestätigung von „Sachverhalten“
  - Z.B. Dokument, Inhalt, Zeitstempel => Hashwert
- DAOs (dezentrale autonome Organisationen)
- IoT, I4.0 …

Usecases – Beispiele 1/3

- Identity & Access Management
  - Bestehende Systeme benötigen vertrauenswürdige zentrale Instanz
  - => Single Point of failure
  - Bei Blockchain Lösungen bekommt „User das Recht auf die Verwaltung der eigenen Identität zurück“
    - Aber gleichzeitig auch die Pflicht!
  - Beispiel Blockstack
    - Namensregistrierung
    - Bindung Namen zu kryptografischem Schlüsselpaar
    - Namensauflösung
    - Alle Funktionen dezentral: Verhinderung von Zensur etc.

Usecases – Beispiele 2/3

- Energiewirtschaft
  - Peer-to-Peer Handel mit Strom
    - Haushalte – Kleinproduzenten (Photovoltaik)
    - Verrechnung direkt über Blockchain
    - Kein „Mittelsmann“: Energielieferant, Bank
    - …
  - Z.B. USA: Brooklyn - „Microgrids“
  - Z.B. D: RWE – Betankung von Elektroautos

Usecases – Beispiele 3/3

- DAOs (dezentrale autonome Organisationen)
  - „Organisation“
    - Keinen physischen Sitz
    - Kein Personal, keinen Chef
    - Nicht registriert
    - => rechtliche Fragestellungen?
  - Basis: Blockchain mit Smart Contracts
    - „programmierte Regeln“
    - „digitale Abstimmung der Aktionäre“
    - „Ausführung der Entscheidungen über die Smart Contracts“
  - Beispiel: Venture Capital für Projekte mit Kryptowährungen (DE/CH)
    - In 3 Wochen 144 Mio USD Anlegergelder gesammelt
    - Aber auch: 50 Mio kurzfristig „verschwunden“ gewesen

Typisierungen von Blockchains

- Scope
  - Public („alle Funktionen von Jedem ohne Erlaubnis nutzbar“)
  - Community (mehrere Unternehmen/Organisationen)
  - Private (unternehmensintern)
- Permission („Mining“: Bestätigung von Transaktionen)
  - Unpermissioned Ledgers (jeder Node kann minen)
  - Permissoned Ledgers (nur ausgewählte Nodes)
- Anonymity
  - Anonym (Pseudonym)
  - Identified
  - (Nicht relevant)

Beispiele für Typisierungen

- Gruppe von Unternehmen in Finanzindustrie
  - Community: mehrere Unternehmen
  - Permissoned: nur ausgewählte Nodes bestätigen Transaktionen
  - Identified: Alle Teilnehmer bekannt
- Bitcoin
  - Public, unpermissioned, anonymous
- Audit-Logs
  - Unternehmensintern, mehrere Systeme
  - „Private“

Next Steps seitens AustriaPro

- Mitarbeit bei TeleTrusT.de – AG Blockchain
  - Positionspapier in Arbeit
- AustriaPro Veranstaltung
  - in Planung
- Synergien zu unseren AK Themen?
  - Identity & Access => USP/WPV

- => Fragen?

Kontakt

AUSTRIAPRO

http://www.austriapro.at
austriapro@wko.at

DI Dr. Christian Baumann
c.baumann@baumann.at
+43 664 43 24 243