Webinar Digitalisierung – Blockchain

Blockchains – (Technische) Grundlagen

AUSTRIAPRO
DI Dr. Christian Baumann

22.5.2018

AUSTRIAPRO

- Standardisierungs- und Expertenplattform - im Umfeld der WKO
- Als Verein organisiert, ca. 70 Mitglieder
- Fachwissen für WKO sowie für UnternehmerInnen
- Arbeitskreise, Pilotprojekte, Veranstaltungen
- Arbeitskreise
  - e-Billing, e-Zustellung, … **Blockchain**
- www.austriapro.at

Inhalt

- Abgrenzung Bitcoin - Blockchain
- Haupteigenschaften
- Kryptografie
- Blockchain
  - Blöcke, Transaktionen, Kette
  - Konsensfindung
  - Ausprägungen
  - Kryptografie – weitere Anwendungen
  - Stärken/Schwächen – Sinn/Unsinn
- Usecases

Disclaimer: Abbildungen Wikipedia (CC0 1.0 oder gemeinfrei)

Abgrenzung Bitcoin / Blockchain

- „Satoshi Nakamoto“: Whitepaper 2008
  - „… elektronischen Währung, die auf einem kryptografischen Beweis beruht und kein Vertrauen in Mittelsmänner benötigt, ist Geld sicher und kann mühelos transferiert werden.“
  - Kernthemen
    - Verteilte Datenbank, P2P Netzwerk
    - Konsens ohne Vertrauen
  - Start Bitcoin Blockchain: Jänner 2009

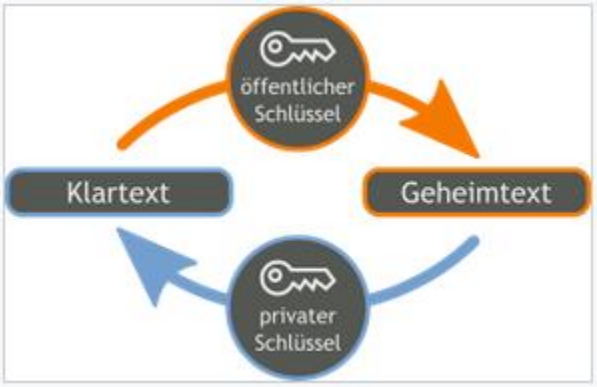
- Bitcoin = Erste Anwendung einer Blockchain
- => Blockchain-Technologie für andere Anwendungen einsetzbar

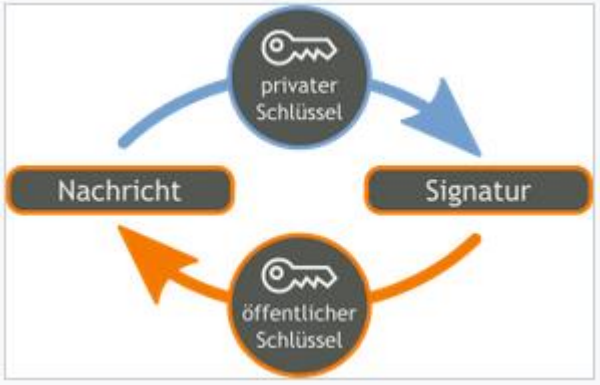
Blockchains - Eigenschaften

- Dezentral
  - P2P (Datenbank, Netzwerk)
  - Robustheit (Ausfallssicherheit)
  - => nicht (bzw. sehr schwer) zerstörbar
- Transparent
  - Konsistente Sicht auf alle Daten
  - Vertrauen durch Kryptografie
- Unveränderbar
  - Neue Daten nur hinzufügen
  - Bestehende Daten unveränderbar/unlöschbar
  - Durch Kryptografie fälschungssicher

Kryptografie 1/2

- Verschlüsselung & digitale Signatur
  - Schlüsselpaar: öffentlicher & privater Schlüssel
    - „asymmetrisch“
  - Verschlüsselung mit öffentlichem Schlüssel des Empfängers
    - Empfänger entschlüsselt mit privatem Schlüssel
  - Digitale Signatur mit eigenem privaten Schlüssel
    - Prüfung mit öffentlichem Schlüssel





Kryptografie 2/2

- Hashfunktionen
  - Digitaler Fingerabdruck von Daten
  - Geringste Änderungen Input => große Änderungen Output
  - Unabhängig von der Länge der Daten
  - Vom Hashwert kann man nicht zu den Daten „zurückrechnen"
  - Eindeutig reproduzierbar

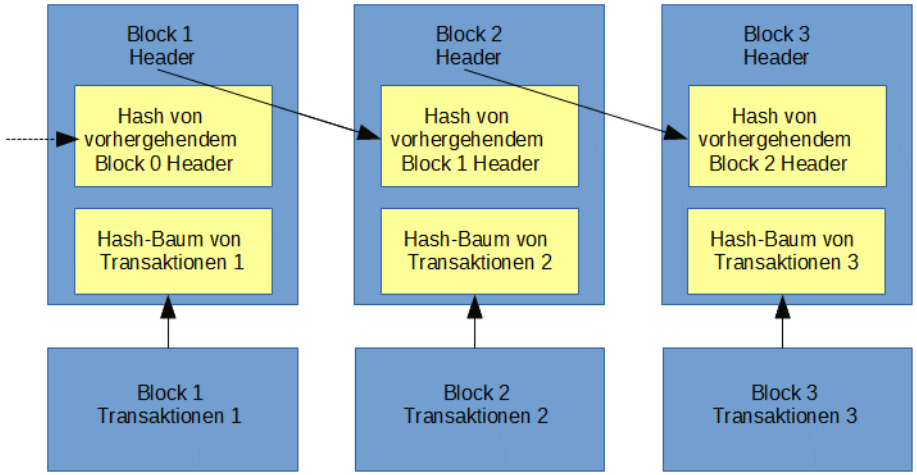
Daten	Hash (sha256)
Kaufpreis EUR 10.000,-	5785f79d6fcff99c1a5ffdbf12518c4c973368e06e3a70cfb87477b32bf8da92
Kaufpreis EUR 10.001,-	55a19ba087c6c32b0cdbe16a5167cf11275615c11feada4bc5b0effc3a236e8f
X	4b68ab3847feda7d6c62c1fbcbeebfa35eab7351ed5e78f4ddadea5df64b8015
Das ist ein langer Text, der Hashwert ist aber trotzdem nicht länger …	0ef31bda0f5fc71152001886cb0e8dc3792565b7df471dcc74ef4fc4bb4c970c

Blöcke & Transaktionen

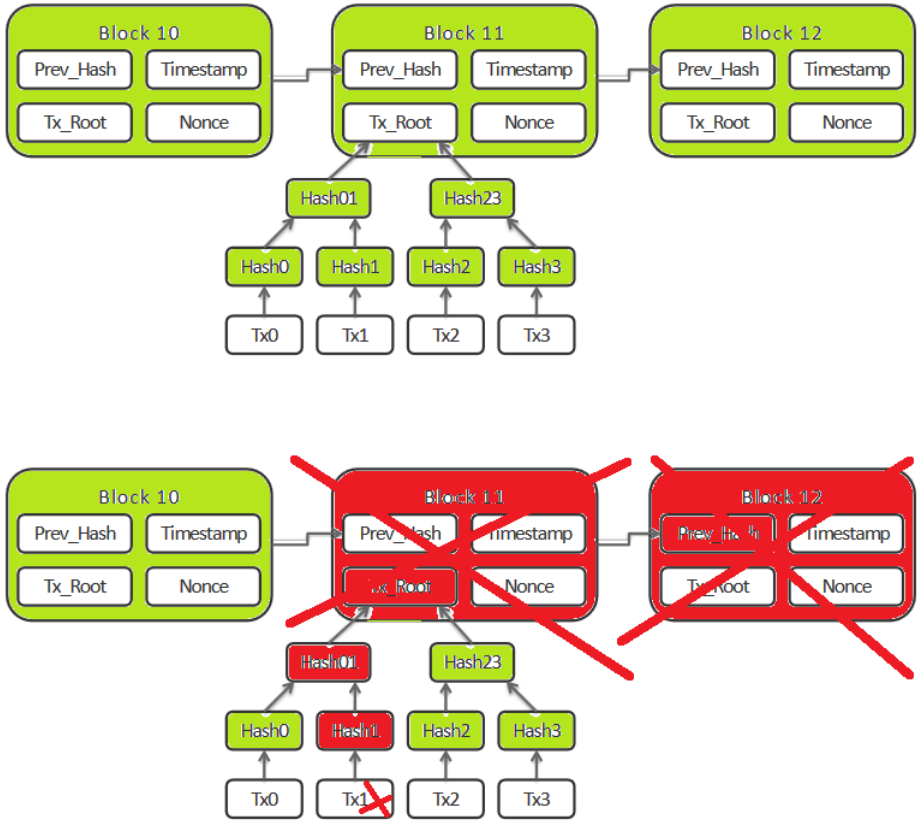
- Datensätze (Blöcke)
  - beinhalten Transaktionen
  - sind kryptografisch abgesichert verkettet
  - neue Blöcke entstehen durch „Konsens“
- Inhalte von Transaktionen
  - Transfer von Werten
    - Vgl. „Überweisungen“ (bei Kryptowährungen)
  - Beliebige andere Informationen oder Daten
    - Klartext, maschinenlesbar, Hashwerte von anderen Daten …
  - „Skripts“
    - Programmcode, u.a. bei Smart Contracts

Blöcke => Kette

- Blöcke
  - bestehen aus Header & Transaktionsteil
    - `Hashwert von Transaktionsteil => Header`
    - `Hashwert von Header => nächster Block`
  - sind kryptografisch abgesichert verkettet
    - `nachträgliche Änderungen „zerstören“ Verkettung`



Manipulierte Daten ...



Konsensfindung

- Genehmigungsprozess für neue Blöcke
  - Neue Transaktionen validieren und in die Blockchain aufnehmen
  - Verteilt (keine zentrale Instanz nötig)
- Erfordert Arbeit („Mining“)
  - „Proof of Work“
    - Rechenintensives Problem => energieintensiv!
    - Größter Kritikpunkt bei Bitcoin (ähnlichen) Blockchains
  - Weitere Verfahren verfügbar bzw. in Entwicklung
    - Proof of Stake, Space, Capacity, Importance …
    - Ibs. für permissioned Blockchains keine hohe Rechenleistung nötig!

Ausprägungen von Blockchains

Je nach Einsatzzweck, 2 Dimensionen

- Zugriff („Wer darf lesen?“)
  - Public: Jeder Client darf (komplette Blockchain) lesen
  - Private: nur bekannte (geprüfte, authentifizierte) Teilnehmer
- Validierung („Wer darf schreiben?“)
  - (Transaktionen verarbeiten, Blöcke bilden und hinzufügen)
  - Permissionless: Jeder Teilnehmer
  - Permissioned: beschränkte Liste („Konsortium-Chain“)

Dimensionsmatrix

		Validierung (schreiben)	
		Permissionless	*Permissioned*
Zugriff (lesen)	*Public*	Bitcoin, Ethereum … PoE, **(öffentlich)**	Register, Zertifikate … **(veröffentlichen)**
	Private	(n/a)	Banken, Versicherungen „Konsortium“ **(intern)**

Kryptografie Anwendung

- Keypairs & Hashverfahren
- Blockchain intern
  - Signieren von Transaktionen
  - Hashwerte der Blöcke => Verkettung
- Zusammenhang mit Daten/Dokumenten
  - Daten
    - verschlüsselt in der Chain speichern
    - nur ausgewählte Empfänger können entschlüsseln/lesen
  - Dokumente
    - „offchain“ transportieren/verspeichern
    - Hashwert als Bestätigung in Blockchain
    - (Speicherplatz, Datenschutz …)

Blockchains - Stärken & Schwächen

- Dezentral
  - Kein Mediator / Intermediär nötig
  - Kein Systembetreiber / Kein Systemverantwortlicher
  - Nicht zensierbar
- Transparent
  - Konsistente Sicht auf alle Daten
  - E2E Verschlüsselung zwischen Teilnehmern möglich
- Unveränderbar
  - Unlöschbarkeit => Datenschutz? (DSGVO)
- Effizienz
  - Höherer Ressourcenbedarf (CPU, Speicher)
  - Geringere Performance (TPS)

Blockchains - Sinn oder Unsinn?

- Einsatz ist wahrscheinlich unsinnig, wenn …
  - Zentrales System (Datenbank etc.)
  - Klarer „Eigentümer“ (der Daten)
  - Firmenintern, konzernintern
  - Teilnehmer bekannt (Vertrauen)
  - Wenige (verteilte) Teilnehmer
  - Hohe Performance nötig
  - Maximale (Daten-)Sicherheit/Vertraulichkeit nötig

Usecases – Beispiele

- Finanzbereich
  - Kryptowährungen, allg. Finanztransaktionen
  - Interbanking Datenaustausch
- „Beweise"
  - Ownership – Nachweis von Besitz (physisch & digital)
  - Notarization – Proof Of Existence (elektronische Dokumente)
  - Asset-Tracking
  - Identity & Access Management
- Industrie, Energie
  - Supply Chain & Logistik
  - (I-) Internet Of Things, Industrie 4.0
  - Energiehandel/-verrechnung
- Öffentlicher Bereich
  - Register (Grundbuch, Firmenbuch …)
  - Zertifikate (Personen, Produkte, CO2 …)
- Smart Contracts
  - dApps
  - ICOs
  - …

Zusammenfassung, Ausblick

- Blockchain Technologien
  - Mehrere Jahre erprobt
  - Stärken/Schwächen, Sinn/Unsinn
  - => Diverse Anwendungsbereiche sinnvoll
- Weitere „Hausaufgaben“ nötig
  - Technische Aspekte
    - U.a. Standardisierung
  - Weitere Rahmenbedingungen
    - rechtlich
    - finanztechnisch, steuerlich
    - politisch

Kontakt

AUSTRIAPRO

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

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