WKÖ, AUSTRIAPRO und Blockchain

Resümee der Gründungssitzung AK Blockchain 30.1.2018

WIRTSCHAFTSKAMMERN ÖSTERREICHS

Programm der Gründungssitzung

- Einleitung - die Blockchain – Sichtweisen von AUSTRIAPRO und WKÖ (Innovation, Information, Standardisierung)

  Dr. Christian Baumann, Dr. Gerhard Laga und Mag. Christian Boser

- Praktische Einführung

  Dr. Christian Baumann

- Einführung in die World Cafe Methode und Kurzpräsentation der einzelnen Themen

  Yvonne Pirkner, Tischmoderatoren

- World Cafe zu Blockchain (4 Tische) samt anschl. Präsentation im Plenum
- kurze Diskussionsrunde zum Arbeitsprogramm 2018 des AK Blockchain

AUSTRIAPRO Grundlagen/Standardisierung

- Ausrichtung & Arbeitsweise

  - Standardisierungsorganisation im Umfeld der WKÖ
  - als Verein organisiert, etwas über 60 Mitglieder
  - Arbeitskreise, Veranstaltungen, Pilotprojekte
  - www.austriapro.at (News, Kontakte, Fachbereiche)
  - NET-WORK Veranstaltungen
  - Arbeitskreise
  - Fachwissen für WKO/WKÖ sowie für UnternehmerInnen

AUSTRIAPRO & Standards

- Welche Bedeutung haben Standards für effiziente Wirtschaftsabläufe?
  - Standards gewähren einfacheren und schnelleren Aufbau von Geschäftsbeziehungen
  - Zusammenwirkung von IT Systemen über Unternehmensgrenzen hinweg, „Interoperabiliät“
  - Standardkonforme E-Business Geschäftsprozesse als Standortfaktor
- Standards entstehen durch gemeinsame Arbeit
  - AUSTRIAPRO entwickelt Standards „bottom-up“ mit den zukünftigen Anwendern, bestes Beispiel ebInterface
  - AUSTRIAPRO arbeitet auf nationaler Ebene mit dem Austrian Standards Institute zusammen, auf europäischer Ebene mit CEN und auf internationaler Ebene mit UN/CEFACT

AUSTRIAPRO & WKÖ E-Center

- Wer macht was?

  - Policy: E-Center (Abstimmung mit WKÖ Abteilungen und Bundessparten)
  - Technologie: AUSTRIAPRO
  - Wissenstransfer (Unternehmer allg.): E-Center (mit E-Day, KMU DIGITAL…)
  - Wissenstransfer (IT Branche, Spezialisten): AUSTRIAPRO

AUSTRIAPRO Arbeitskreise

- Arbeitskreise 2018
  - E-Billing
  - Austausch elektronischer Rechnungen, direkte Kommunikation zwischen FiBu Systemen, ebInterface Standard
  - E-Zustellung
  - gesicherte und nachweisbare Zustellung elektronischer Dokumenten (E-Einschreiben), auch im Rechtsbereich (TrustNet)
  - Wirtschaftsportalverbund
  - gemeinsam elektronische Identitäten (eID) sicher verwalten
  - allgemeines Regelwerk für eID Management (WPV Rulebook)
  - Umsetzung von Use Cases (z.B. Compass Verlag)
  - neu: Blockchain

Blockchain Arbeitskreis

- Ziele
  - Information (z.B. bei welchen Geschäftsprozessen ist die Blockchain sinnvoll?)
  - Diskussion (Einsatzgebiete, Chancen, Risiken, nationale und internationale Entwicklungen)
  - Testbed (Labs) für gefahrloses Ausprobieren von Blockchain Anwendungen
  - Pilotprojekte (welche effizienten und sicheren Einsatz der Blockchain Technologie vorzeigen)
  - Erarbeitung von Standards, wo nötig

- Nicht- Ziele
  - Blockchain allgemein „promoten“
  - einzelne Lösungen favorisieren
  - das Thema Kryptowährungen

Blockchain – WKÖ Sicht

- Expertenwissen soll national aufgebaut
- eventuell nationale Infrastruktur etablieren, soferne nötig
- Abstimmung mit Bundesministerium für Digitalisierung und Wirtschaftsstandort bzw. dessen Blockchain Agenda
- Was kann die WKO in eine Blockchain einbringen?
- Austauschplattform für interessierte Unternehmen anbieten
- Kommunikation der Chancen und Risiken an alle Mitglieder (digital.now und eventuell KMU DIGITAL 2019+)

Blockchains – technische Grundlagen

- Abgrenzung Bitcoin - Blockchain
- Haupteigenschaften
- Kryptografie
- Blockchain
  - Blöcke, Transaktionen, Kette
  - Konsensfindung
  - Ausprägungen
  - Kryptografie Anwendungen
- 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.“
  - Implementierung 2009
  - Kernthemen
    - Verteilte Datenbank, P2P Netzwerk
    - Konsens ohne Vertrauen

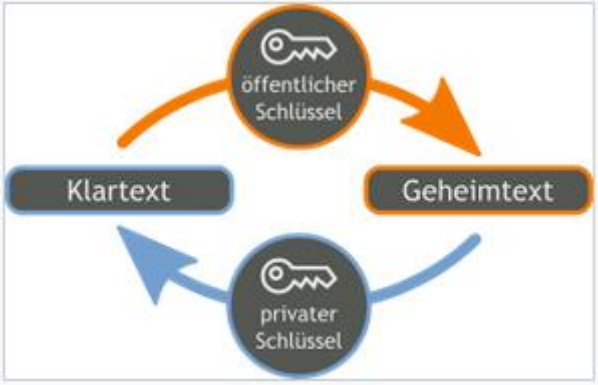
- Bitcoin = 1. (verbreitete) Anwendung einer Blockchain
- …
- => Blockchain-Technologie für andere Anwendungen

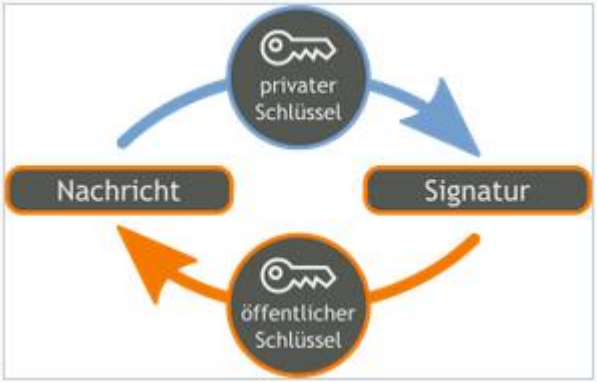
Haupteigenschaften der Blockchain-Technologie

- Dezentral
  - Technisch: Datenbank, Netzwerk, kein Single Point of Failure
  - Organisatorisch: Keine Intermediäre (Vermittler, Banken …)
  - => nicht zerstörbar, zensierbar
- Transparent
  - Peer-to-Peer Struktur
  - => alle haben konsistente Kopie der Daten
- Fälschungssicher
  - Neue Daten können nur im neuen (nächsten) Block hinzugefügt werden
  - Bestehende Daten können nicht mehr verändert, gelöscht … werden

Kryptografie (1 von 2)

- Verschlüsselung
  - 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 von 2)

- Hashfunktionen
  - Digitaler Fingerabdruck von Daten
  - Geringste Änderungen Input => große Änderungen Output
  - Vom Hashwert kann man nicht zu den Daten zurückzurechnen

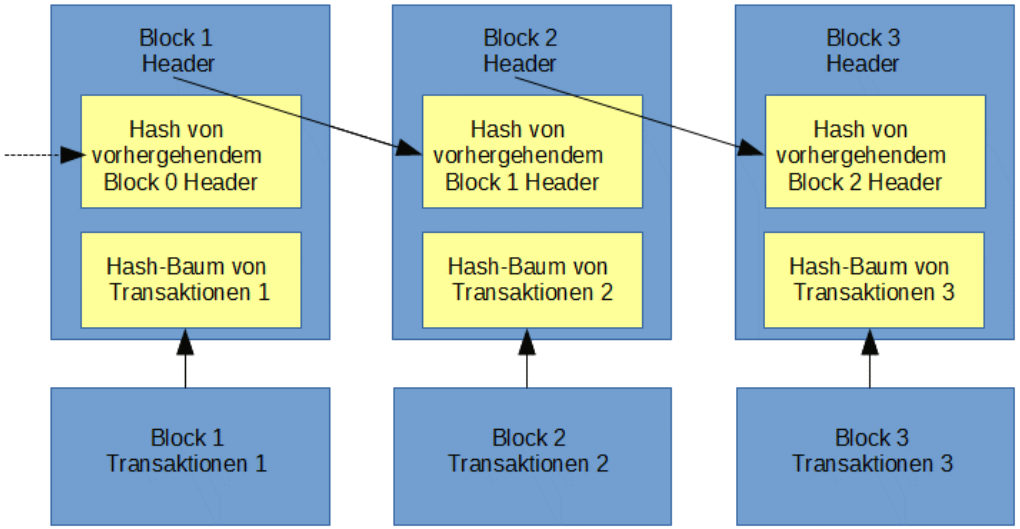
Daten	Hash (sha256)
Kaufpreis EUR 10.000,-	5785f79d6fcff99c1a5ffdbf12518c4c973368e06e3a70cfb87477b32bf8da92
Kaufpreis EUR 10.001,-	55a19ba087c6c32b0cdbe16a5167cf11275615c11feada4bc5b0effc3a236e8f

Blöcke & Transaktionen

- Datensätze (Blöcke)
  - beinhalten Transaktionen
  - sind kryptografisch abgesichert verkettet
  - neue Blöcke entstehen durch „Konsens“
- Inhalte von Transaktionen
  - Transfer von Werten (bei Kryptowährungen), vgl. Überweisungen
  - andere Informationen oder Daten (Klartext, Hash)
  - „Skripts“ (Programmcode), Smart Contracts

Blöcke => Kette

- Blöcke
  - bestehen aus Header & Transaktionsteil
  - sind kryptografisch abgesichert verkettet
    - nachträgliche Manipulationen „zerstören“ Verkettung



Konsensfindung

- Genehmigungsprozess für neue Blocks
  - Neue Transaktionen validieren und in die Blockchain aufnehmen
    - Z.B. Missbrauch erkennen (Double Spend …)
    - Auch „Spam“, DoS … erkennen/verhindern
  - 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, zwei 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 („Consortium-Chain“)

Dimensionsmatrix

		Validierung (schreiben)	
		Permissionless	*Permissioned*
Zugriff (lesen)	*Public*	Bitcoin, Ethereum … PoE, (öffentlich)	Register, Zertifikate … (veröffentlichen)
	Private	(n/a)	Banken, Versicherungen … (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 (PoE)
    - (Speicherplatz, Datenschutz …)

Use Cases - Beispiele

- Zahlungen, Kryptowährungen, allg. Finanztransaktionen
- Ownership – Nachweis von Besitz (physisch & digital)
- Notarization – Proof of Existence
- Identity & Access Management
- Asset-Tracking
- Supply Chain & Logistik
- Internet of Things, Industrie 4.0
- Energiehandel/-verrechnung
- Diverse Register (Grundbuch, Firmenbuch …)
- Diverse Zertifikate (Personen, CO_2 …)
- Smart Contracts, ICOs …

Vorstellung der World Cafe Methode

- Kurzinfo: **Wie funktioniert ein World Cafe?**
- Unsere **Thementische:**
  - **Tisch 1: Allgemeines & Technik**
  - **Tisch 2: Transportlogistik**
  - **Tisch 3: Zertifizierungen**
  - **Tisch 4: Weitere Themen**
  - **Output**

    Pro Thementisch werden zum Abschluss 5 relevante Erkenntnisse/Ideen/Diskussionspunkte im Plenum vorgestellt

Input für die „Reise“ (World Cafe)

- **Fokus auf das, was wichtig ist**
- **Eigene Ansichten und Sichtweisen beitragen**
- **Ideen verlinken und verbinden**
- **Sprechen und Hören mit Herz und Verstand**
- **Hinhören, um wirklich zu verstehen**
- **Jeder versorgt seine eignen Ideen**
- **Aufmerksamkeit auf die Entdeckung neuer Erkenntnisse und tiefergehender Fragen**
- **Spielen, kritzeln, malen**
- **Haben Sie Spaß dabei!**

Reisebegleitung (Fokus World Cafe)

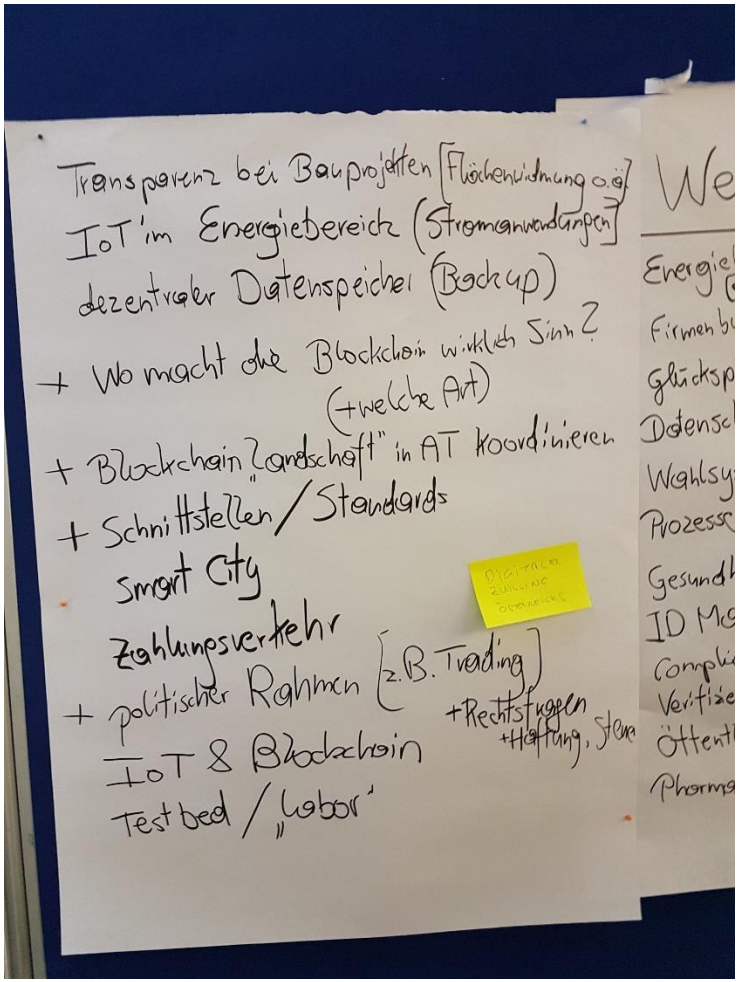
- Diskussion/Ideen zu Möglichkeiten für den **Einsatz der Blockchain-Technologie**
- Diskussion/Ideen zur **Testumgebung**, in der **unterschiedliche Technologien ausprobiert** werden können
- Diskussion/Ideen für **Pilotprojekte**, die den **effizienten** und **sicheren Einsatz der Blockchain-Technologie** aufzeigen

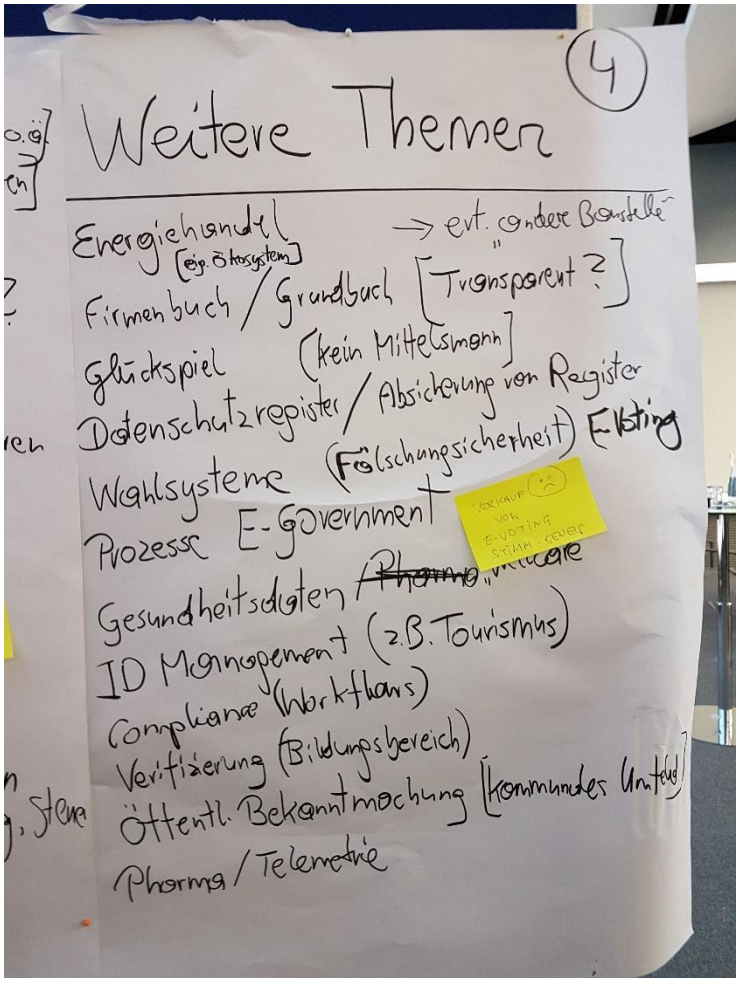
Fotoprotokoll „Allgemeines & Technik“

Fotoprotokoll „Transportlogistik“

Fotoprotokoll „Zertifizierungen“

Fotoprotokoll „Weitere Themen“





Zusammenfassung „Allgemeines & Technik“ (1 von 3)

- Allgemeines
  - Entscheidungshilfe
    - „Wann soll man BC-Technologie einsetzen, wann nicht?“
    - Was sind typische Einsatzszenarien?
    - Liste/Vergleich diverser Blockchainvarianten (auch im Hinblick auf Energieverbrauch)
  - Wissen & Bildung forcieren!
    - Firmen, die BC Projekte haben, zu Erfahrungsberichten einladen
    - Infos über Beispielprojekte z.B. blockchainpilots.nl
  - Es sollte ein „Gütesiegel“ für BC related Firmen geben, ähnlich wie „e-Commerce Gütesiegel“, ev. mit besonderem Augenmerk auf ICOs.

Zusammenfassung „Allgemeines & Technik“ (2 von 3)

- Technik / Lab
  - Kompatibilität von Blockchains!?
  - Proof of …; Vergleiche, auch hinsichtlich Skalierung
  - Die Rolle des Miners (ibs. in nicht Kryptocoin Anwendungen
  - Statements:
    - Usersicht: Frontends werden immer wichtiger und bringen den eigentlichen Mehrwert; Userinterface: „wie soll eine BC App entworfen werden?“
    - Art und Weise Software zu entwickeln, wird sich massiv ändern
    - Das Finden von BC-erfahrenen Entwicklern ist derzeit fast unmöglich
    - Dogma „User = Node“ hinterfragen, => User <> Node
  - Sicherheit
    - Wie wird sich diese in Zukunft entwickeln? Neue Algorithmen? (z.B. quantum-proof?)
    - Hardware Ebene? Z.B. Intel SSE, Smart Meters …
    - Sichere Cloud als „Anker“ für Smart Contracts
  - Lab
    - verschiedene (gängige) Technologien nötig
    - Schnittstellen zwischen BCs?
    - Praktische Erfahrungen?

Zusammenfassung „Allgemeines & Technik“ (3 von 3)

- Anwendungen
  - Zeiterfassung/-verrechnung für Personal, ibs. in dezentralen (multinationalen) Organisationen
  - Smart Contracts für „Prüfung“ physischer Lieferungen: Empfänger bestätigt Erhalt, SC „zahlt Rechnung“
  - Automatisierte Verifikation von Smart Contracts
  - BC-basierende Wahl, am Beispiel WK-Wahl
  - Protokollierung von Zugriffen auf sensible Daten (z.B. lt. DSGVO)
  - Asset Tracking
  - E-Zustellung (iSv Dokumentenübermittlung) mit Smart Contracts
  - Nachverfolgung von Workflows, z.B. in e-Government Systemen (vgl. Projekt BMF mit Multichain)
  - Industrie: Anlage wird durch Blockchain/SmartContracts „gesteuert“, fertige (und korrekte) Teile werden sofort „bezahlt“.

Zusammenfassung „Zertifizierungen“ (1 von 2)

- Verwaltung durch/über Zertifikate
  - für Subunternehmer z.B. im Baubereich
  - für Mitarbeiter z.B. Sicherheitsunterweisungen
  - die Unternehmen bei Banken beibringen müssen
  - im Universitätsbereich für Stipendienverwaltung
- Ausstellung
  - von Arbeitszeugnissen
  - Referenzen von Aufträgen z.B. im Vergaberecht öfter notwendig
- Branchenspezifische Zertifikate:
  - Umweltfreundliche Technologien z.B. grüner Wasserstoff
  - Bio Chemie, chemische Elementzertifikate
  - Güter erfüllen Eigenschaften/Normen
  - Seriosität/Gütesiegel von Dienstleistungen und Produkten
- Betreiberübergreifende Bestätigungen für mobiles Lernen
- Frage der Granularität des Zugriffes: darf jeder das ganze Zertifikat mit verschiedenen Bereichen (z.B. Semesterzeugnis) sehen? Betroffener soll Einzeldaten freigeben, eventuelle Lösung über „ZK Snark“

Zusammenfassung „Zertifizierungen“ (2 von 2)

- EU-Lösung vs. nationalen Lösungen: EU Vorsitz nutzen!
- elektronische Dokumentzustellung/Ausweispflichten erledigen
- ZMR-Vereinswesen-Human Life Cycle Management
- Staatlich verliehene Befähigungen z.B. Führerschein, Waffenschein
- Staatliche Zuordnungen z.B. Grundbuch, E-Residence (Estland), Visa
- Wer zertifiziert Sprachen/Software-Versionierungen/IT-Systeme?
- Zertifikate für Prozessoren/Sensoren und deren Software iZm IoT und Updates
- Zertifikate für Connected Driving (Auto/Motorrad Komponenten)

Zusammenfassung „Weitere Themen“

- Register (Firmenbuch, Grundbuch, Datenschutzregister…)
- Blockchain Landschaft in AT (beschreiben/koordinieren)
- Gesundheitsdaten/Pharma/Telemetrie
- dezentraler Datenspeicher
- IoT & Blockchain (u.a. im Energiebereich)
- Einsatz in der öffentlichen Verwaltung/E-Government Prozesse
- Schnittstellen/Standards/Kompabilität
- Security Themen
- E-Voting/fälschungssichere Wahlsysteme
- Infrastruktur die Smart City
- Zahlungsverkehr (Dokumentation)

Zusammenfassung „Transportlogistik“ (1 von 2) Einsatzbereiche

- Dokumentenmanagement, z.B.
  - Frachtpapiere zur Verarbeitung und Dokumentation in BCs abwickeln
  - automatische Zollabfertigung durch Integration von Behörden
- Tracking & Tracing, z.B.
  - BC als Instrument zur Nachverfolgung und Dokumentation von Arbeitsschritten/Aktivitäten entlang der logistischen Kette
  - von sicherheitsrelevanten Produkten/Modulen, z.B. im Flugzeugbau oder im medizinischen Bereich
- Marktplätze, z.B.
  - für freie Transport-, Lager- und Produktionskapazitäten
  - Ermöglichung von Sharing-basierten Geschäftsmodellen mit Peer-to-Peer Charakter
- Asset Management, z.B.
  - Aufzeichnung von Fahrzeugeinsatzdaten (elektronischer Fahrtenschreiber)
  - Dokumentation von Unfällen (Zertifikat/BC-Pass für Fahrzeuge, B2B und B2C)

Zusammenfassung „Transportlogistik“ (2 von 2) Herausforderungen/Aufgaben

- Identifizierte Herausforderungen
  - Komplexität und technische Handhabbarkeit
  - Eignung von BC-Technologie für jeweiliges Einsatzszenario
    - technisch
    - betriebswirtschaftlich (Kosten-Nutzen-Verhältnis)
  - derzeit fehlende Standards
  - Skalierbarkeit der Lösung
  - parallele Entwicklung inkompatibler Blockchains
  - Qualität von Daten, die von Personen / Sensoren generiert werden
- Aufgaben
  - Identifizierung von betriebswirtschaftlich und technisch sinnvollen Use-Cases
  - Identifizierung von Ansätzen zur Verknüpfung unterschiedlicher BCs
  - Schaffung von Sandboxes als sichere Testumgebungen
  - Schaffung von Standards und „Rulebooks“

Ergänzung - allgemeine wichtige Fragen/Themen

- Welche Formen der Blockchain gibt es und wann sollte welche Form für ein Unternehmen zum Einsatz gebracht werden?
- Wie kann ein Unternehmen herausfinden, welche Daten sinnvoll in die Blockchain geschrieben werden können (und welche nicht)? Welche Partner brauche ich dazu, die mir die Infrastruktur aufbereiten bzw. die die Daten nutzen können?
- Identifikation von verschiedenen Business Cases für Unternehmen bzw. Branchen
- Modellierung der Blockchain, damit ersichtlich wird, wie die Blockchain in das Unternehmen wird (Datenmodelle, Prozessmodelle, Geschäftsmodelle …)

Wie geht es weiter?

- Themenauswahl seitens der AUSTRIAPRO Geschäftsstelle in Abstimmung mit WKÖ E-Center
- Vertiefung der ausgewählten Themen
- Vorbereitung der Bildung von Arbeitsgruppen innerhalb des Arbeitskreises
- Vorbereitungen zum Test-Bed und in Sachen Pilotprojekte

- Der nächste Arbeitskreistermin ist der 13.3.2018, 15-17 Uhr, WKÖ Saal 2

Danke und Kontakte/Infos

Kontakte:

- Dr. Christian Baumann: c.baumann@baumann.at (speziell Technik)
- Dr. Gerhard Laga: gerhard.laga@wko.at (speziell Recht)
- Mag. Christian S. Boser christian.boser@wko.at (speziell organisatorische Fragen)
- für allgemeine Anfragen: austriapro@wko.at

Weitere Informationsquellen:

- wko.at/blockchain
- www.austriapro.at (Schlagzeilen, Veranstaltungen…)