Arbeitskreis Blockchain

Allgemeines & Arbeitsgruppe Technik & Blockchain Lab

Dr. Christian Baumann

30.6.2020

AUSTRIA PRO

Inhalt

- News zu „Austrian Public Service Blockchain”
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab
- Blockchain-basiertes Immunitätszertifikat
- open space – Projekte, Initiativen, Informationen
  - Zoltan Fazekas
  - Sascha Mundstein – „PIA – Prove It All“
  - Christoph Zinganell - „Token4Hope“
  - weitere Meldungen (spontan)

AUSTRIA PRO

Austrian Public Service Blockchain („APSB“)

- Initiative von Institutionen der öffentlichen Verwaltung
- Aufbau einer „Konsortium-Blockchain“ für unterschiedliche Usecases im „public service“ Bereich
  - Blockchain in Echtbetrieb seit 10/2019
- Konsortialpartner derzeit
  - BRZ (Bundesrechenzentrum)
  - Gemeinde Wien
  - WKO (Wirtschaftskammer)
  - Nic.at (cert.at)
- NEU (zugesagt)
  - Kontrollbank
  - WU Wien
- Weitere
  - TU Wien, FH St. Pölten

AUSTRIA PRO

Status und next steps

- Austrian Public Service Blockchain
  - Vereinbarung zwischen den drei „Gründern“
    - Basierend auf Portalverbundvereinbarung
    - Aktuell in Fertigstellung (nächster Termin 1.7.2020)
  - Weitere Partner aus öffentlichen Verwaltung aufnehmen
  - Weitere Usecases definieren
- Daten-Zertifizierung WKO
  - Seit 12/2019 in Echtbetrieb
  - Externes Verifikationsservice
    - auch für nicht „mein.wko.at“ User
    - und zur Verifikation von Dokumenten anderer Services
  - Ergänzung QR-Code mit Direkt-Link zu Verifikationsservice

Externes Verifikationsservice

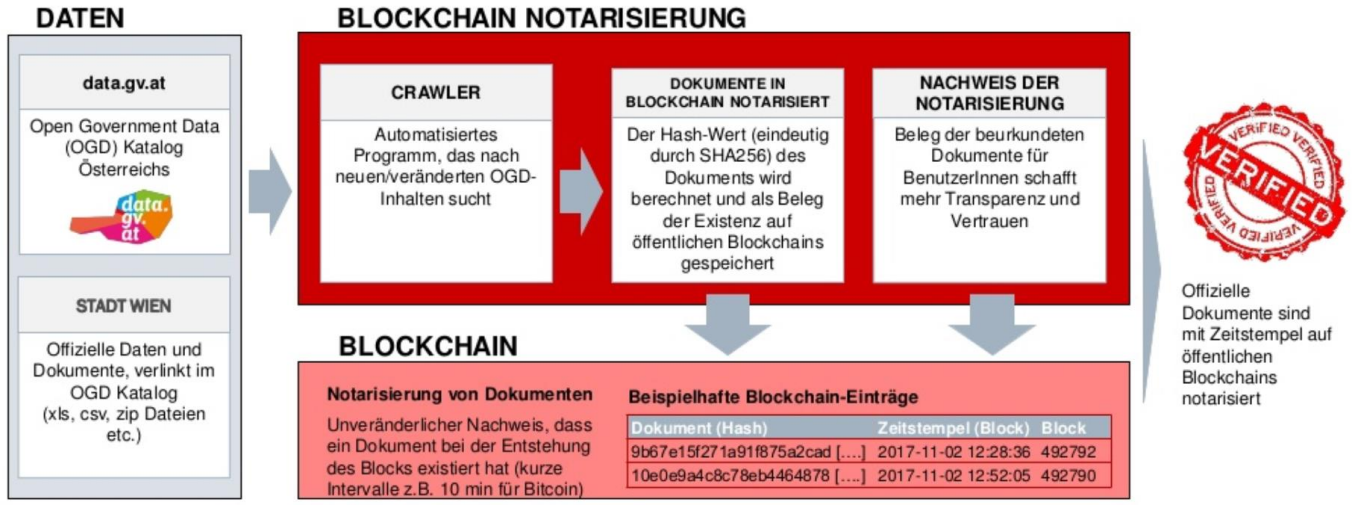
- https://datenzertifizierung.at/verify/ oder
- https://daten-zertifizierung.at/verify/

- ev. zukünftig „Dual-Verify“?

AUSTRIA PRO

APSB – Wien – OGD Notarisierung

- Absicherung der Integrität von Open Government Data durch Hashwerte in einer Blockchain
  - Dezember 2017: 1. Blockchain-Pilot
  - Aktuell: Umbau Blockchain Infrastruktur auf APSB
  - https://www.slideshare.net/DigitalesWien/1-blockchainpilot-der-stadt-wien-ogd-notarization



"Daten Zertifizierung" auf Basis Blockchain - Gutachten

- Privatgutachterliche Stellungnahme
  - Dr. Knasmüller (allg. beeideter & ger. zertif. Sachverständiger)
- Inhalt
  - Beschreibung System und Funktionsweise
  - Verwendete Technologien & Standards
- Publiziert am 6.3.2020 - https://www.wko.at/service/netzwerke/gutachten-daten-zertifizierung-auf-basis-blockchain.pdf

Der damit beauftragte gerichtlich zertifizierte Sachverständige Dr. Markus Knasmüller stellt zusammenfassend fest:

Es ist daher von einer verlässlichen Möglichkeit, zu beweisen, dass elektronische Daten zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert haben und seither nicht verändert wurden, auszugehen.

➔ Wg. Nachfrage: Gilt analog für APSB & privatwirtschaftlichen Bereich!

AUSTRIA PRO

„Datenzertifizierung“ für die Privatwirtschaft

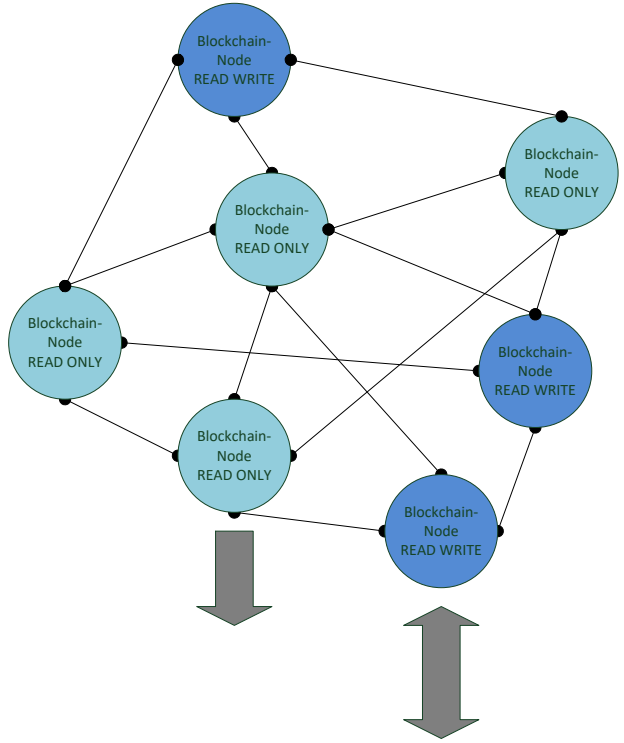
- Basis APSB => Diverse Anfragen aus Privatwirtschaft
- WKO/AUSTRIAPRO
  - „Unterstützung einer privaten Konsortialblockchain zur Zertifizierung von Daten”
  - **Zielsetzung: Aufbau einer dauerhaften und sicheren Blockchain-Infrastruktur für Österreichs Wirtschaft**
  - Einrichtung und Moderation eines offenen Stakeholder-Forums zum Aufbau und Steuerung der Infrastruktur
    - Kooperation ABC und AustriaPro (WKO)
    - Projekt gestartet (siehe eigene Folien)

- Klarstellung
  - Kein Mitbewerb zu APSB, sondern “Schwesternsystem”
  - Kommende Synergien (z.B. gemeinsames Verify)

AUSTRIA PRO

„Datenzertifizierung“ für die Privatwirtschaft

- Systemaufbau
  - Dieselbe technologische Basis wie APSB
  - Einfachere Regeln als im öffentlichen Bereich
  - Funktionale Erweiterungen je nach Anforderungen
  - Ausprägung als Konsortiumchain
    - Vertrauenswürdige Unternehmen & Institutionen betreiben die Blockchain Nodes (Schreibzugriff)
    - Öffentlicher Lesezugriff (Read-Only Nodes) zum Validieren der Daten



AUSTRIA PRO

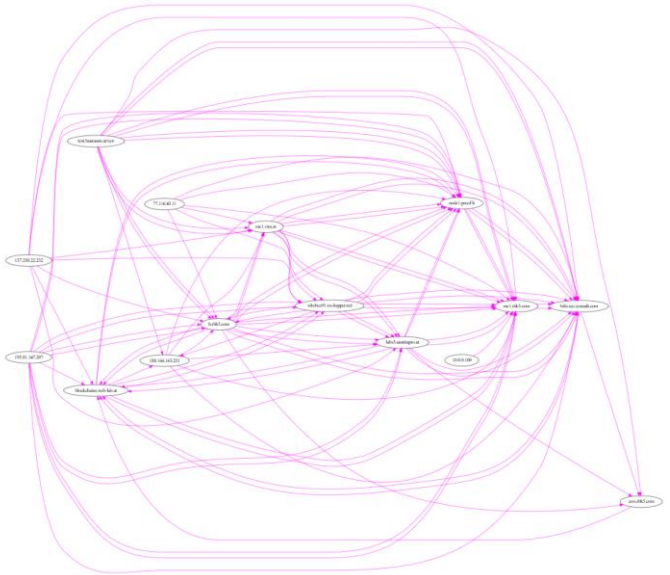
„Datenzertifizierung“ für die Privatwirtschaft

- Kosten
  - Kosten für Node
    - Setup & Betrieb
    - Keine Lizenzkosten für Node selbst
  - Keine „Transaktionskosten“
  - Geringe „Verwaltungsgebühr“
    - z.B. Vereinsmitgliedsbeitrag
- Mögliche neue Services für Provider
  - „Blockchain as a Service“ oder
  - „API as a Service“

AUSTRIA PRO

Status & Next Steps 1/2

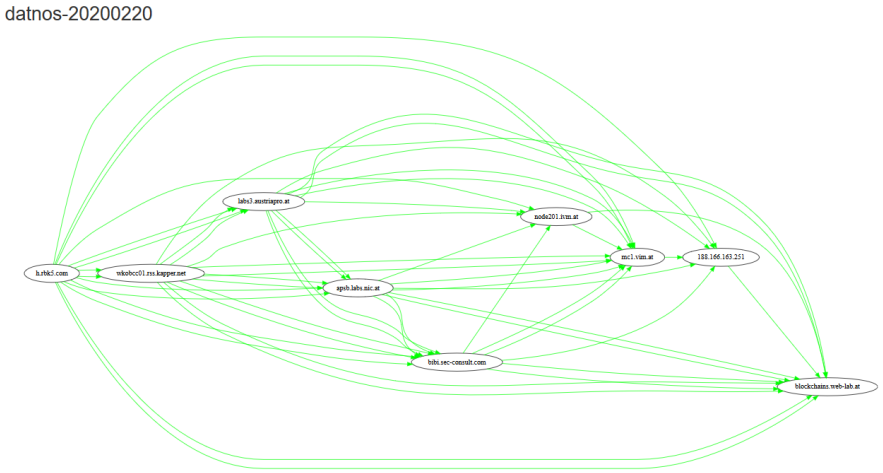
- Testsystem
  - Seit >> 1,5 Jahren verfügbar
  - u.a. auch im Blockchain-Lab
  - vgl. Libraries/Demos (github)
    - https://github.com/austriapro/blockchain
  - Ca. 15 Teilnehmer (Test-Nodes)
  - Ca. 10 weitere Teilnehmer (über APIs)



Status & Next Steps 2/2

- Echtsystem (Blockchain) gestartet am 20.2.2020
  - Dzt. 8 + 2 Teilnehmer
  - Parallel zur „Einrichtung ... eines offenen Stakeholder-Forums“
  - => Forschungsprojekt mit ABC

  - Erste Anwendungen demnächst live
  - => Moderation einstweilen durch AustriaPro



AUSTRIA PRO

AUSTRIAPRO / ABC Projekt - „Distributed Ledger Technology (DLT) and Data Protection Law”

Forschungsfragen: **Rechtliche und organisatorische** Rahmenbedingungen einer Konsortialblockchain, die von Unternehmen und Privatpersonen nach Akzeptanz eines Vertrages eingehalten werden sollen.

- Welche Besonderheiten sind zu beachten, damit eine solche Blockchain-Infrastruktur nicht in Konflikt mit den Anforderungen der **DSGVO** kommen kann? (Können Hashwerte personenbezogene Daten sein und wenn ja, welche Konsequenz hat das?)
- Wie kann die **Governance** gestaltet sein, damit ein solches System für möglichst viele Teilnehmer offen ist, aber gleichzeitig destruktives oder rechtsverletztes Verhalten hintanhält/verunmöglicht/verbietet (also für ein ausgewogenes Verhältnis zwischen Stabilität und Innovation sorgt)?
- Welche **Sicherheitsanforderungsmodelle** können zum Einsatz kommen für den direkten Zugang zur Blockchain und dem Zugang zu darauf aufbauenden blockchainbasierten Anwendungen?
- Wie kann die **Eigentümerschaft an Daten** oder der Blockchaininfrastruktur entstehen bzw. vermieden werden und wie können Modelle für die Regelung aussehen?
- Welche Modelle können eine dynamische **Weiterentwicklung** der Blockchain-Infrastruktur technologisch, von den zugrunde gelegten Regelungen, aber auch von Anwendungsseite sicherstellen und gleichzeitig negative Entwicklungen verhindern?
- Wie können **Business Modelle** für den Betrieb einer solchen Blockchain-Infrastruktur aussehen, die eine faire Kostenverteilung gewährleisten.

AUSTRIA PRO

Teilnehmer – Private Sector Blockchain

Private Sector Blockchain (Nodes)	Node test	**Node produktiv**
AUSTRIAPRO	ja	**ja**
baumann.at - concepts & solutions	ja	**ja**
block42 Blockchain Company GmbH	ja	**ja**
NIC.at GmbH		**ja**
RBK5.com	ja	**ja**
SEC Consult Unternehmensberatung GmbH	ja	**ja**
VIM Internet GmbH	ja	**ja**
WKO - Wirtschaftskammer Österreich		**ja**
NEU		
IVM Technical Consultants GmbH	ja	**setup**
Securikett Ulrich & Horn GmbH	ja	**setup**

AUSTRIA/PRO

Neue Teilnehmer – Private Sector Blockchain

- IVM Technical Consultants GmbH
  - Personalmanagement und TestCenter in den Bereichen technische und kommerzielle Software- und IT-Solutions, Elektronik & Elektrotechnik, Maschinenbau & Anlagenbau
  - 4 Standorte in Österreich
  - 200 technische ExpertInnen
  - Blockchain Usecases
    - Software Development, Build Prozess, Bestätigung für Versionsstände etc.
    - …

Neue Teilnehmer – Private Sector Blockchain

- Securikett Ulrich & Horn GmbH
  - Führendes Unternehmen im Bereich Produkt- und Markenschutz
  - Physikalischer und digitaler Produktschutz (Manipulationsschutz)
  - 80 Mitarbeiter, Export in 45 Länder
  - Blockchain Usecase: Batcherstellung im Pharmabereich
    - Daten: Produktnummer, Charge, Haltbarkeitsdatum, Seriennummern …
    - Protokollierung der Daten/-änderungen im „Audit-Trail“
    - Überprüfung und Nachweis der Unverfälschtheit der Daten
    - (Gestartet als TIP Förderprojekt der WK-NÖ)
    - Parallelbetrieb mit zweiter Blockchain (BLUchain, Schweiz)

Blockchain-Lab

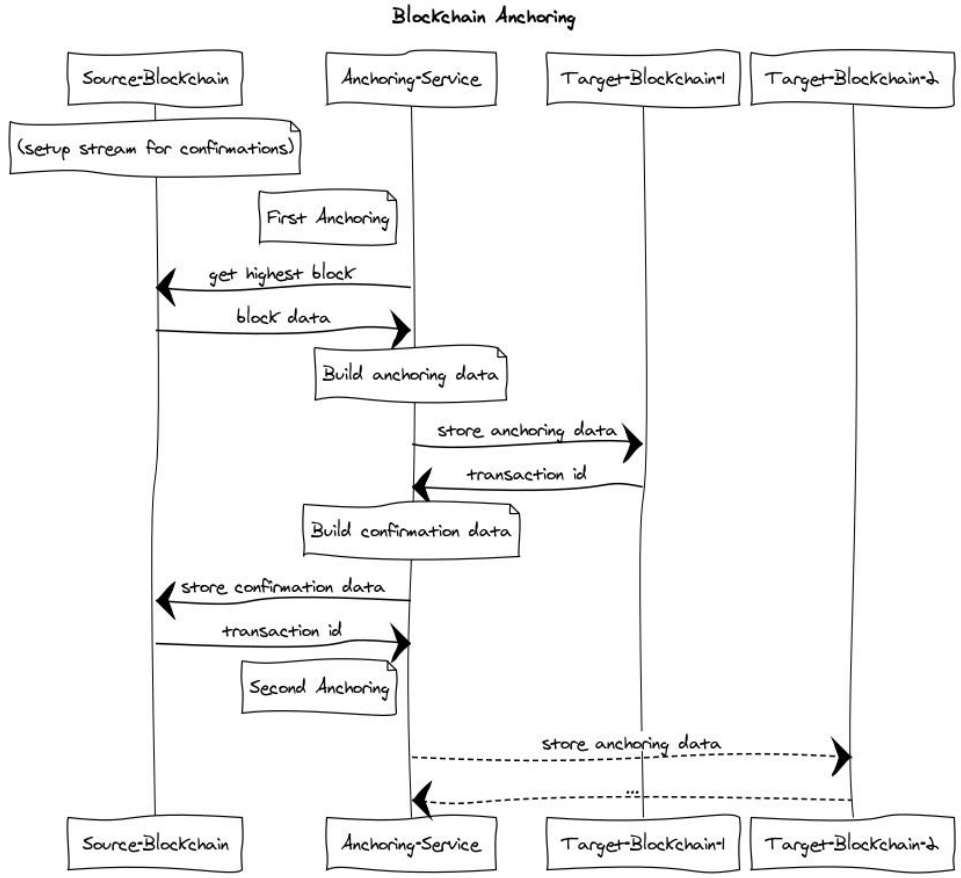
- Thema Anchoring

Anchoring

- Notarisierung des aktuellen Zustandes einer (z.B. privaten oder Konsortium-) Chain in public Blockchains
- D.h. potentielle Manipulationen in einer „kleinen“ Chain werden verhindert (bzw. würden erkannt)
- Zustands-Daten
  - Aktueller Block
    - Blocknummer
    - Hash
    - Zeitstempel
  - …

Anchoring - Ablauf

- Anchoring Service bereitet Daten einer Source-Blockchain auf und
- trägt sie in ein oder mehrere Target-Blockchains ein.
- Bestätigung wird in Source-Chain eingetragen



Anchoring

- Beispiele für Target Chains

3. Welche Target Chains?

Target-Blockchain	Anzahl an (Full-) Nodes	Kosten pro Transaktion
Bitcoin	10.000	€ 0,50
Ethereum	12.000	€ 0,10-0,30
...		
Artis	...	...

- Aktueller Status
  - Prototypische Implementierung gestartet
  - Neu: immer noch nicht fertig ;-)

AUSTRIA PRO

Blockchain-basiertes Immunitätszertifikat 1/4

- Projekt „Immunitätsnachweis“
  - WKO => ABC-Research
  - Parallel zu Projekt „Safe A“
  - Dzt. 1. Phase: Anforderungen, Marktanalyse, Rahmenbedingungen
- Fokus
  - Zuverlässiges, sicheres und datenschutzkonformes System für digitale Gesundheitszertifikate
    - Ersatz von bzw. Ergänzung zu bisher verwendeten Papier Bestätigungen
    - Basierend auf dezentraler & Blockchain Technologie
  - Initialer Usecase
    - Immunitätsstatus (Antikörpertests)
    - Impfbestätigungen (sobald verfügbar)
    - Andere Testergebnisse (z.B. PCR)

AUSTRIA PRO

Blockchain-basiertes Immunitätszertifikat 2/4

- Herausforderungen
  - Medizin: Zuverlässigkeit der Tests, Dauer/Ausmaß der Immunität, Impfungen …
  - Ethik/Recht: Gefahr einer „Zwei Klassen Gesellschaft“, Freiwilligkeit, Diskriminierung …
  - Organisation: Integration aller Stakeholder, Schutz gegen Mißbrauch, Akzeptanz, internationale Interoperabilität(!)
  - Technik: Systemarchitektur, Sicherheit, Skalierbarkeit …

Blockchain-basiertes Immunitätszertifikat 3/4

- Umfeld
  - International 30+ Projekte zu COVID 19 Immunitätsnachweisen
    - z.B. Restart.ID 1 , Open University 2 , Ubirch 3 , Covid Credentials Initiative 4
  - Kritische Diskussion zu möglichem Nutzen und Risiken
    - WHO 5 , Harvard 6 , Nature 7 , Lancet 8 , JAMA Network 9 , Stanford 10 , Standard 11

- 1 https://www.staatsdruckerei.at/news/schneller zur normalitaet restart id konzept fuer digitale immunitaetskarte/
- 2 https://blockchain.open.ac.uk/#covid 19
- 3 https://corona gesundheitszertifikat.de/
- 4 https://www.covidcreds.com/
- 5 https://www.who.int/news room/commentaries/detail/immunity passports in the context of covid 19
- 6 https://ethics.harvard.edu/immunity certificates
- 7 https://www.nature.com/articles/d41586 020 01451 0
- 8 https://www.thelancet.com/journals/lancet/article/PIIS0140 6736(20)31034 5/fulltext
- 9 https://jamanetwork.com/journals/jama/fullarticle/2765836?utm_campaign=articlePDF&utm_medium=articlePDFlink&utm_source=articlePDF&utm_content =jama.2020.8102
- 10 https://law.stanford.edu/2020/04/10/covid 19 immunity certificates practical and ethical conundrums/
- 11 https://www.derstandard.at/story/2000118161716/forscher warnen erneut vor covid 19 immunitaetspaessen

AUSTRIA PRO

Blockchain-basiertes Immunitätszertifikat 4/4

- Möglicher Lösungsansatz
  - Zertifizierte Stelle (z.B. Labor) erstellt Immunitätsnachweis
    - Durch digitale Signatur der ausgebenden Stelle bestätigt
    - User speichert Zertifikat „unter eigener Kontrolle“ (z.B. am eigenen Smartphone)
    - Hinterlegung von fälschungssicheren Prüfsummen („Hashes“) in Blockchain
  - Überprüfung erst nach Zustimmung durch den User möglich(!)
    - Prüf App kontrolliert
      - Gültigkeit des geteilten Zertifikats selbst (Signatur, falls möglich)
      - Prüfsumme in der Blockchain
  - Evtl. Abstraktion der Testergebnisse durch vorgegebene Policies
    - z.B. Corona Impfung in anerkanntem Labor im letzten Jahr => grüner Status

Projekt „Safe A“

- Dzt. wichtigste strategische Projekt für Wirtschaftsstandort Österreich
- BMLRT (Landwirtschaft, Regionen, Tourismus) mit WKÖ
- Ziel: Sicherer Urlaub in Österreich
  - Regelmäßige und flächendeckende präventive Testung der Mitarbeiter der Tourismusbetriebe (wöchentlich)
- Organisation
  - Pilotphase (Juni): 5 Regionen (Wilder Kaiser, Montafon, Wachau, Spielberg, Wörthersee), Ausbau bis 20k Tests/Woche
  - Echtbetrieb (ab Juli): ca. 65k Test/Woche
- Ganzheitliche Prozesskette (Abstrich, Transportlogistik, Befundübermittlung …)
  - Konsortium aus privaten Labors

AUSTRIA PRO

- open space – Projekte, Initiativen, Informationen
  - Zoltan Fazekas
  - Sascha Mundstein – „PIA – Prove It All“
  - Christoph Zinganell - „Token4Hope“
  - weitere Meldungen (spontan)

Vielen Dank für Ihre Aufmerksamkeit.

www.austriapro.at

austriapro@wko.at

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