Arbeitskreis Blockchain
Arbeitsgruppe Technik & Blockchain Lab

AUSTRIAPRO

Dr. Christian Baumann

20.11.2019

Agenda

- Allgemein
  - Austrian Public Service Blockchain
  - „Datenzertifizierung“ für die Privatwirtschaft
  - Rechtliches Gutachten
- Lab
  - Phase 6 Ergänzung
  - Phase 7
    - Self Sovereign Identity
    - IoT Identity
  - Weitere Themen
- News

Austrian Public Service Blockchain

- Initiative von Institutionen der öffentlichen Verwaltung
- Aufbau einer „Konsortium-Blockchain“ für unterschiedliche Usecases im „public service“ Bereich
- Beteiligte (Gründung)
  - BRZ (Bundesrechenzentrum)
  - Gemeinde Wien
  - WKO (Wirtschaftskammer)
- Weitere
  - WU Wien, TU Wien, FH St. Pölten
  - Cert.at, ev. UNO

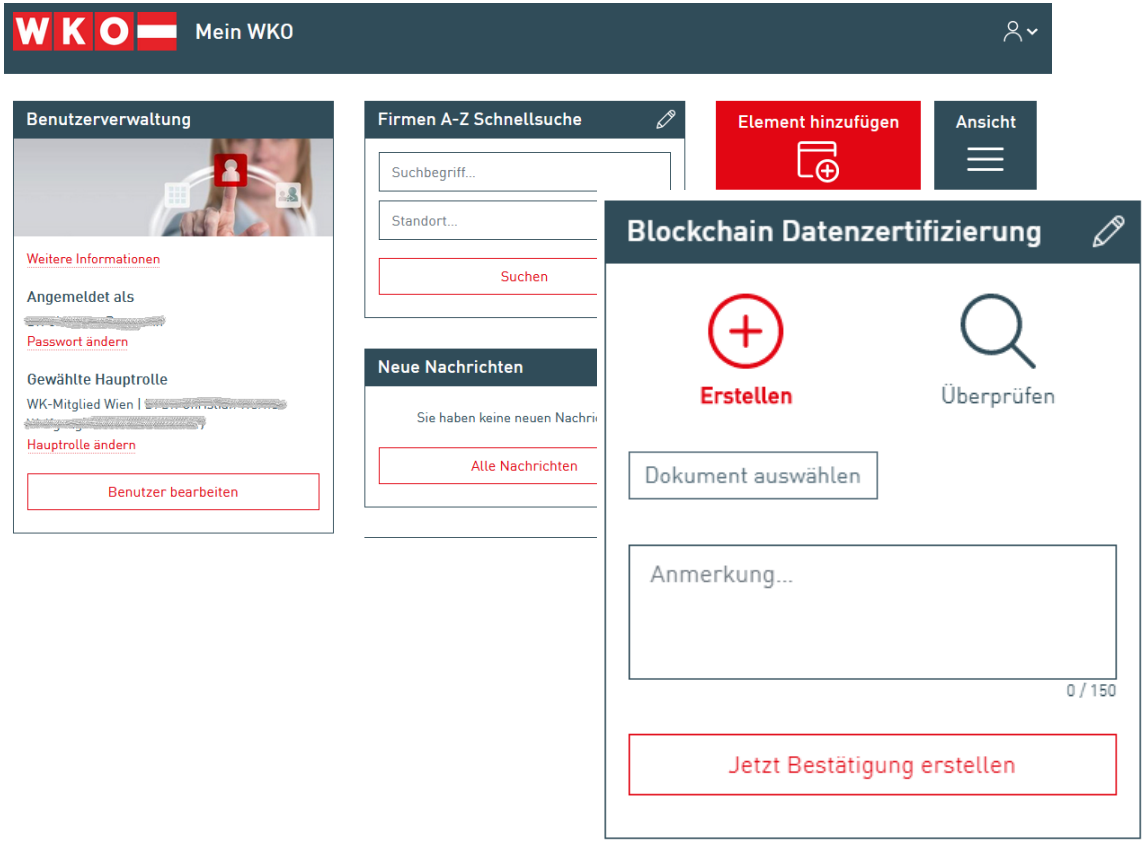
1. Usecase: Notarisierung

- Notarisierung
  - Mit Notarisierung kann bewiesen werden, dass ein elektronisches Dokument zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert hat und seither nicht verändert wurde.
  - Die Sicherheit und das Vertrauen, dass hinterlegte Daten nicht manipuliert werden können, werden dabei durch die Blockchain-Technologie gewährleistet.
  - Es werden ausschließlich anonyme Daten verarbeitet!
    - Hashwerte von elektronischen Dokumenten
    - (ggf. technische Infos)
    - KEINE personenbezogenen Daten

WKO „Daten-Zertifizierung“

- Anderer Begriff für „Notarisierung“
- Blockchainumgebung siehe „APSBC“
  - Echtbetrieb seit Oktober 2019
- Integration GUI in mein.wko erledigt
- Echtbetrieb seit 6.11.2019
  - Dzt. für WKO intern, d.h. alle Mitarbeiter
  - Demnächst für WKO Mitglieder

GUI im Dashboard „mein.wko.at“



Status und next steps

- Austrian Public Service Blockchain
  - Vereinbarung zwischen den drei „Gründern“
    - Basierend auf Portalverbundvereinbarung
  - Weitere Partner aus öffentl. Verwaltung aufnehmen
  - Weitere Usecases definieren
    - Z.B. Liste der Public Keys von PVP (Idee Wien)
- Daten-Zertifizierung WKO
  - „externes“ Verifikationsservice
    - auch für nicht „mein.wko“ User
    - und zur Verifikation „anderer“ Dokumente
  - Echtbetrieb auf WKO-Mitglieder ausweiten

„Datenzertifizierung“ für die Privatwirtschaft

- Bereits mehrere Anfragen aus Privatwirtschaft
- WKO/AP: „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 bzw. Organisation**
  - **Kooperation ABC (WU Wien) und AustriaPro (WKO)**
  - WKO betreibt Blockchain-Knoten (aktuell Testsystem)

„Datenzertifizierung“ für die Privatwirtschaft 1/2

- Systemaufbau
  - Dieselbe technologische Basis wie „Daten-Zertifizierung“
  - Einfachere Regeln wie 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

„Datenzertifizierung“ für die Privatwirtschaft 2/2

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

Next Steps

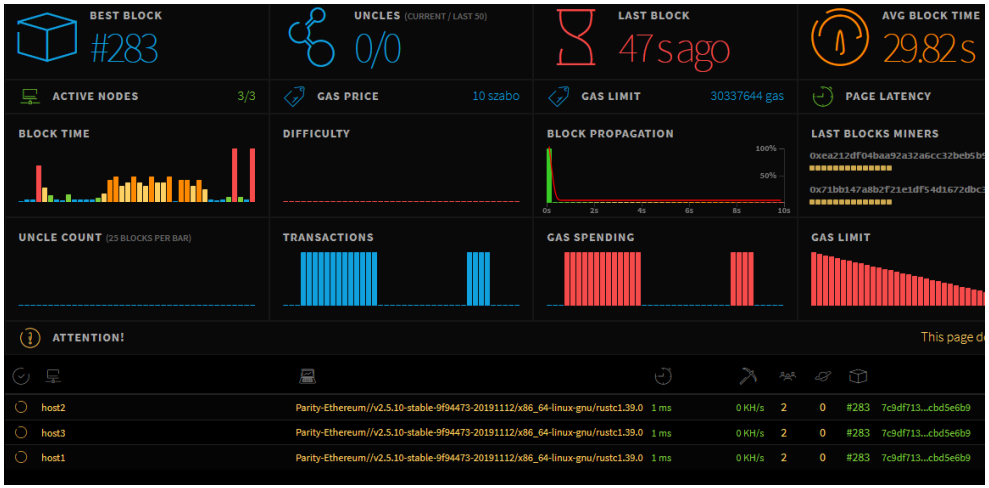
- Testsystem
  - Verfügbar (u.a. auch im Blockchain-Lab)
    - Ein paar Unternehmen betreiben bereits Test-Nodes
  - Technisch konsolidieren (abstimmen)
- Organisation
  - AustriaPro und Austrian Blockchain Center
    - (AustriaPro wird Partner des ABC)
  - Definition Forschungsprojekt
    - Rechtliche und organisatorische Rahmenbedingungen
- Echtsystem
  - Ab wann sinnvoll/nötig?
  - Parallel zu Forschungsprojekt?

"Daten Zertifizierung" auf Basis Blockchain - Gutachten

- Privatgutachterliche Stellungnahme
  - Dr. Knasmüller (allg. beeideter & ger. zertif. SV)
- APSBC & private Anwendungen
- Geplanter Inhalt
  - Beschreibung System und Funktionsweise
  - Verwendete Technologien & Standards
    - Multichain; Opensource ...
    - Hashwertberechnungen lt. mindestens SHA-2/256 oder SHA-3
  - Praktische Versuche
    - im Rahmen des AUSTRIAPRO Blockchain Labs
  - Ggf. Verbesserungsvorschläge
    - "Verständnis"

Lab - Phase 6: „Ethereum V2“ - Ergänzung

- Ethereum Proof Of Authority Chain
  - 3 Nodes, 1 Dashboard
  - Verfügbar im Lab
    - Für Developer: Freischaltung Firewall erforderlich
  - Docker Image zum selbst betreiben
    - Incl. Setupanleitung



Lab - Phase 7: „SSI“

- Self Sovereign Identity
  - Vgl. Network #16
- Neue Module/Systeme im Lab bereitstellen
  - Aktuell: Installation Sovrin „Steward“
    - Z.B. verwendet von https://meinesichereid.org/
    - Konsortium (Banken, Telekom …)
    - Branchenübergreifendes, offenes Trust-Netzwerk …
- Next Steps?
  - Demos?
  - Schnittstellen?

Lab - Phase 7: „IoT-Identity“ 1/2

Blockchain-basierte digitale Identitäten für IoT Devices

- Use-case
  - Blockchain Anwendungen müssen mit der Außenwelt kommunizieren, z.B.
    - z.B. (Sensor-)daten erfassen
    - Aktoren ansteuern
  - Entweder über definierte Nodes oder über „Oracles“
- Problemstellung
  - Daten müssen „vertrauenswürdig“ sein, d.h.
  - 1) Sensoren/Aktoren geprüft, geeicht … nach entsprechenden Normen
  - 2) jeweils eigene eindeutige Identität (unfälschbar, unmanipulierbar)

Lab - Phase 7: „IoT-Identity“2/2

- Lösungsansatz
  - (IoT-) Devices mit Kryptofunktionen (Public-Key Kryprografie)
  - Können eigene Identität
    - bereitstellen (Key-Pairs generieren) und
    - beweisen (digitale Signatur)
  - Teilweise bereits (am Markt) verfügbar
- Schwerpunkte im Projekt
  - Demonstration der gesicherten und vertrauenswürdigen Integration solcher Devices in Blockchain Anwendungen
  - Verwaltung der digitalen Identitäten der Devices
    - Kooperation mit Arbeitskreis WPV (Identity für Unternehmen)
  - Dissemination

Beispiel: Devices mit Kryptofunktionen

- Infineon „Blockchain Security 2Go“ Starterkit
  - Hackathons 2019 Graz / Villach
  - Topic „notarization and proof for geo based games“ (e.g. geocaching)
  - Concept & prototype blockchain solution
    - `Check in riddles`
  - Check & notarize („proof“) the first solver & physical finder
- „Daten aus der Außenwelt … gesichert in die Blockchain“
- Beispielcode etc. => ins Lab einbringen

Blockchain Lab – Weitere Themen 1/2

- Artis Blockchain
  - lab10 collective (Graz)
  - Focus e-mobility solutions
  - Im Lab: Node im Testnetz
    - http://status.tau1.artis.network/
  - Geplant: Validator-Node im Echtsystem
    - https://artis.eco/

Blockchain Lab – Weitere Themen 2/2

- „Anchoring“: Zusätzliche Absicherung von (privaten/Konsortium) Chains mit Hilfe von State-Notarisierung in public Blockchains
  - Incl. prototypischer Implementierung

- Ergänzung Homepage!

News

- IoT & Digitalisierung Fachkonferenz (14.11.2019)
  - Präsentation über AustriaPro Blockckain Lab

Kontakt

AUSTRIAPRO

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

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