Arbeitskreis Blockchain

Allgemeines & Arbeitsgruppe Technik & Blockchain Lab

Dr. Christian Baumann

9.12.2020

AUSTRIA PRO

Inhalt

- News zu „Austrian Public Service Blockchain”
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab
- open space – Projekte, Initiativen, Informationen
  - „Gretchenfrage: Wie vertrauenswürdig ist Blockchain-Technologie?“, Klaus Veselko, cis-cert
  - “Status Blockchain Trade Platform (BTP)“, Andreas Luxbauer & Ergun Türker
  - weitere Meldungen (spontan)

Austrian Public Service Blockchain („APSB“) - Status 12/2020

- Initiative von Institutionen der öffentlichen Verwaltung
- „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: WU Wien - Blockchain-Node & Notarisierung in Echt-Betrieb**
- Zugesagt
  - Kontrollbank (zugesagt)
- Weitere (angefragt)
  - FH St. Pölten, TU Wien …

AUSTRIA PRO

Austrian Public Sector Blockchain – Aktuelle Teilnehmer

Austrian Public Sector Blockchain (Nodes)	Node Test	**Node Produktiv**
BRZ (Bundesrechenzentrum)	ja (2)	**ja (2)**
Stadt Wien - MA01	ja (2)	**ja**
WKO (Wirtschaftskammer Östrerreich)	ja	**ja**
nic.at/cert.at	ja	**ja**
WU (Wirtschaftsuniversität Wien)	ja	**ja**
AUSTRIAPRO	(ja)	

AUSTRIA PRO

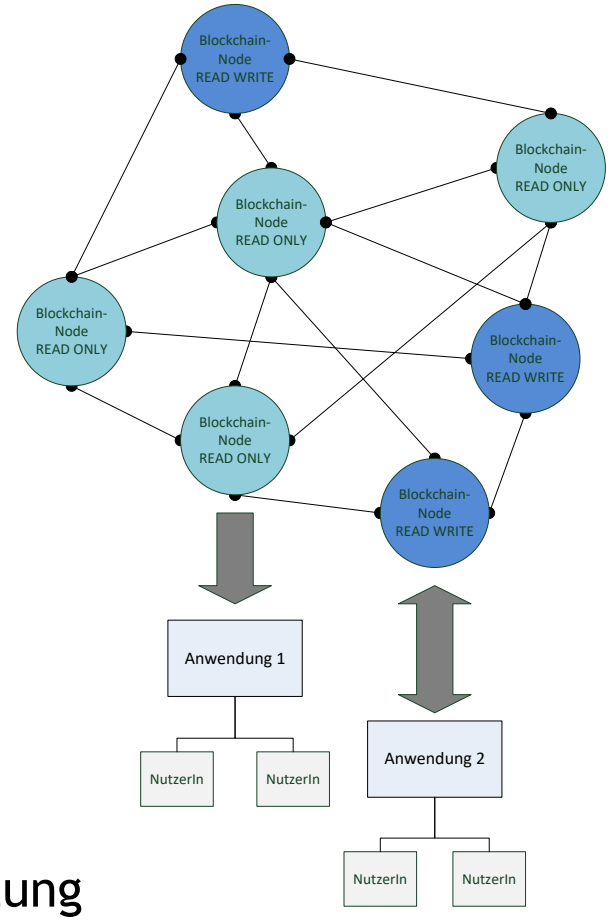
Austrian Public Service Blockchain (APSB) Vereinbarung

- **„Vereinbarung über die einzuhaltenden Rahmenbedingungen bei der Einrichtung und Betrieb eines Austrian Public Service Blockchain-Knotens“**
- Projektgruppe
  - AutorInnen von Stadt Wien, WKO, AustriaPro, BRZ
  - Unter Mitarbeit von ÖKB, WU/ABC, eGIZ, BMDW
- Status: Dokument (inhaltlich) fertig: v0.9c => BLSG
- „E-government Empfehlung“
  - https://reference.e-government.gv.at
  - … die gemeinsam erarbeiteten Vorschläge der Arbeitsgruppen und die daraus resultierenden Konventionen in Form von "Empfehlungen" und "Informationen" publiziert …

AUSTRIA PRO

Austrian Public Service Blockchain (APSB) Vereinbarung

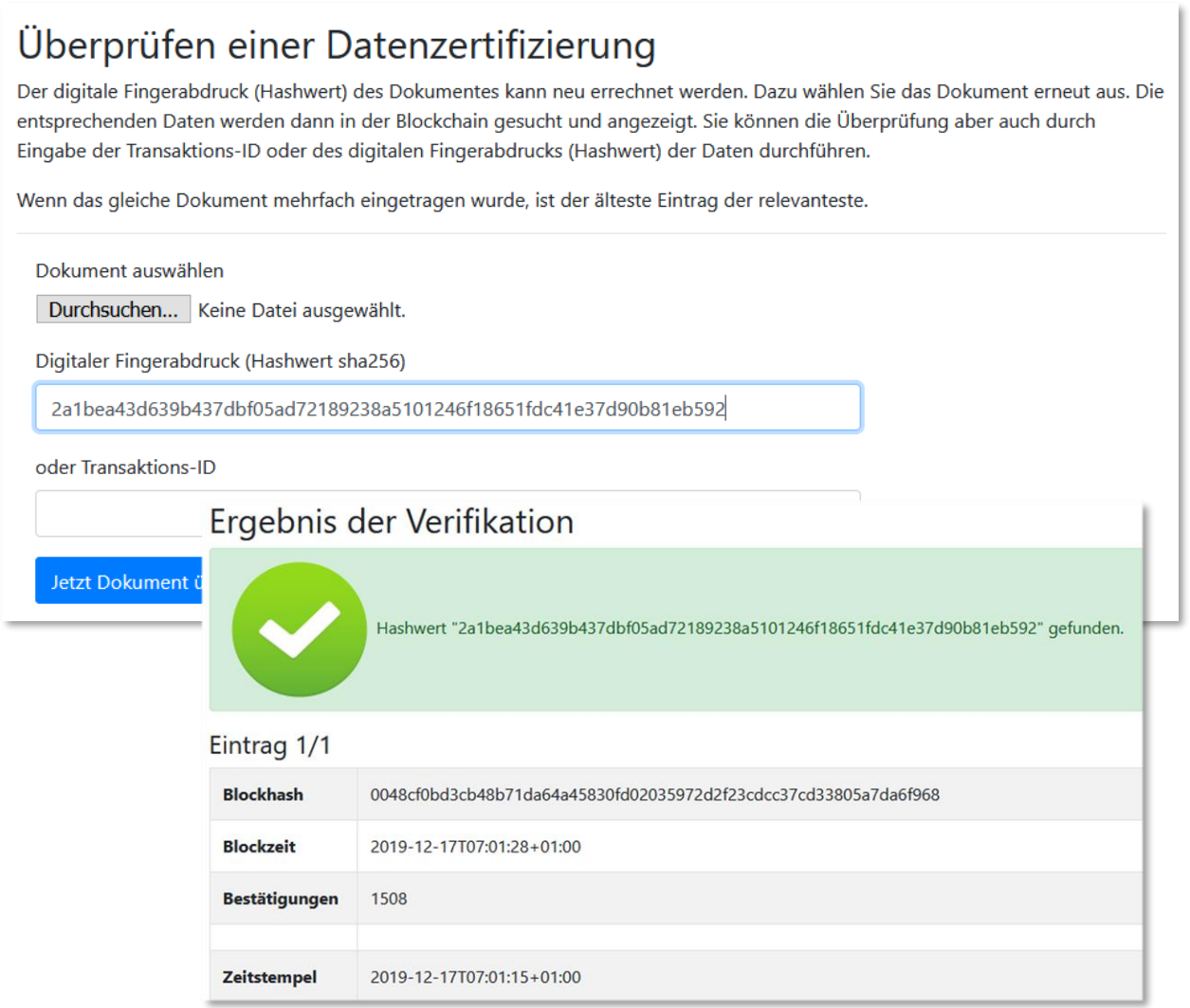
- Inhalt
  - Gegenstand und Zweck
  - Architektur
  - Begriffsbestimmungen
  - Beitritt zur APSB
  - Rechte und Pflichten von Anwendungsverantwortlichen
  - Rechte und Pflichten der Knotenverantwortlichen
  - Technische und organisatorische Vorkehrungen
  - Haftungsregelungen
  - Entzug der Teilnahme
  - Änderungen der Vereinbarung über die APSB
- Anhänge
  - Beitrittserklärung
  - Technische Spezifikation
  - Kooperationsvereinbarung zur gemeinsamen Weiterentwicklung



AUSTRIA PRO

WKO: Zusätzliches „externes“ Verifikationsservice

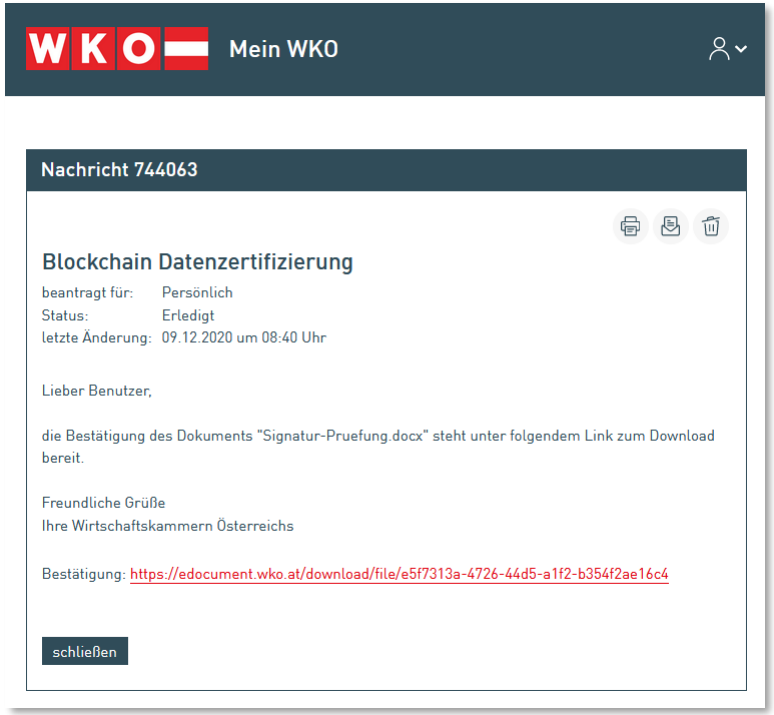
- https://daten-zertifizierung.at/verify/
- Anwendung
  - auch für nicht „mein.wko.at“ User
  - zur Verifikation von Dokumenten, die von anderen Services (**WU, Wien**) zertifiziert wurden
  - Neu: auch durch QR verlinkt
  - zukünftig ev. „Dual-Verify“ – auch Dokumente der Private-Sector Blockchain



WKO Daten-Zertifizierung - NEWS

Bestätigung überarbeitet

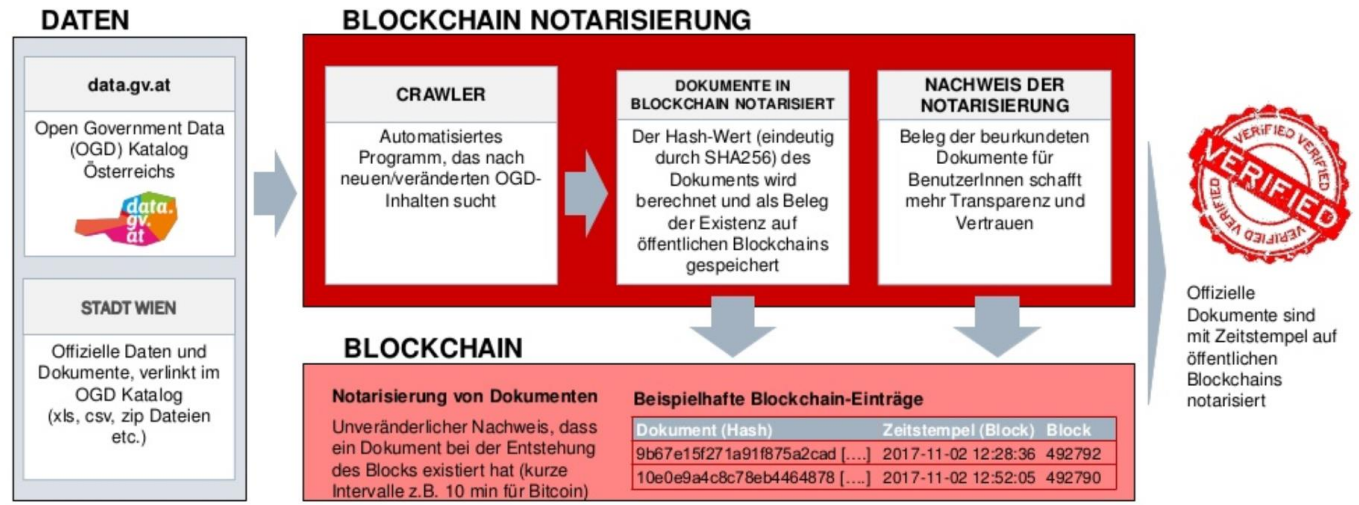
- Erläuterungen
- QR-Code zu Verifikationsservice



APSB – Wien – OGD Notarisierung

Absicherung der Integrität von Open Government Data durch Hashwerte in einer Blockchain

- Dez. 2017: 1. Blockchain-Pilot
- Aktuelles Projekt: Umbau der Blockchain Infrastruktur auf APSB
- Status
  - MA01 betreibt (dzt. 2) Nodes in der APSB
  - Anwendung soeben in Umstellung
- **Ziel: Echtbetrieb 12/2020**



https://www.slideshare.net/DigitalesWien/1-blockchainpilot-der-stadt-wien-ogd-notarization

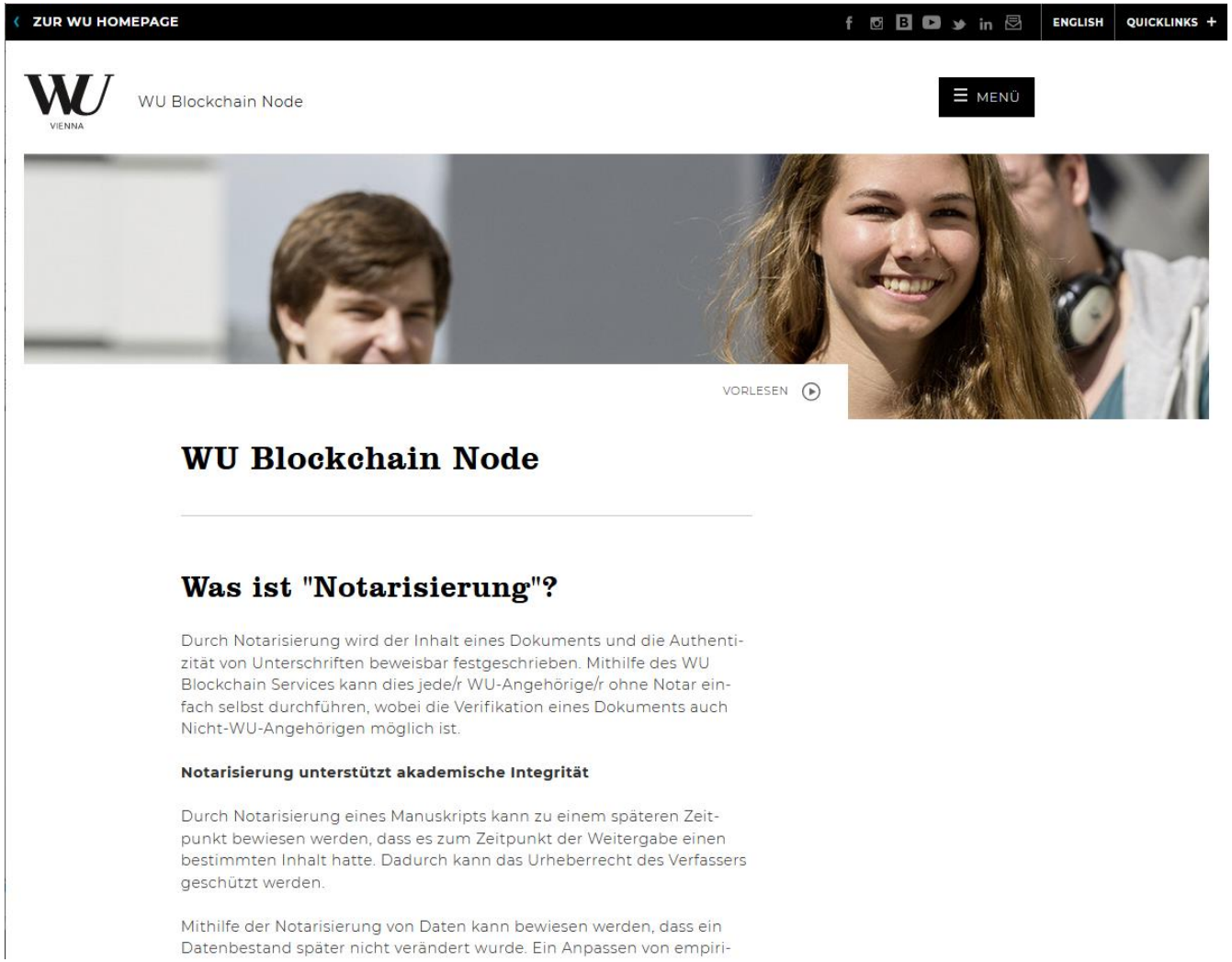
AUSTRIA PRO

APSB – WU (Wirtschaftsuniversität Wien)

- Neuer Teilnehmer per 9/2020
- Echtbetrieb seit Anfang 12/2020, Veröffentlichung Mitte 12/2020
- Use-Case Notarisierung – Akademische Integrität
  - Manuskripte – Urheberrecht des Verfassers
  - Daten – Datenbestand nicht verändert (kein Anpassen von empirischen Erhebungen an Hypothesen)
  - Zeugnisse, Bestätigungen und Zertifikate (auch ohne Amtssignatur)
- Organisatorisches
  - Notarisierung erstellen – nur aus WU internem Netz (bzw. VPN)
  - Notarisierung verifizieren – auch aus öffentlichem Netz
    - Verifikation natürlich auch für alle anderen Dokumente von WKO, Wien … und umgekehrt

AUSTRIA PRO

https://www.wu.ac.at/blockchain/



AUSTRIA PRO

Home \ Notarisierung erstellen

Notarisierung erstellen

Zum Erstellen einer Notarisierung wählen Sie bitte ein Dokument aus. Die Datei wird dabei nicht auf den Server hochgeladen, sondern der Hashwert wird lokal im B

Datei auswählen (wird NICHT auf den Server geladen):

Durchsuchen... WorkingPaper_KT_20201129_v09.pdf

Berechneter Hashwert (sha256):

07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c0516

Dateiname (*):

WorkingPaper_KT_20201129_v09.pdf

Anmerkung (optional, *):

Projekt KT, Analyse, V0.9

(*) als Information, wird NICHT in der Blockchain gespeichert.

Erstellen

Nach dem Eintragen der Informationen in die Blockchain werden die Erg (Zeitstempel, Transaktions-ID ...) angezeigt und können in Form einer Bes Datei) heruntergeladen werden.

Ergebnis der Erstellung

Notarisierung erstellt.

Die Notarisierung wurde erfolgreich erstellt, Details sind in der folgen und können als PDF-Datei heruntergeladen werden (siehe Link unten

Zeitstempel	2020-11-29T11:04:48+01:00
Hashwert	07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c05166
Transaktions-ID	212bf6a226764812e31f42d0733d625a43e6cd201476cf2b0ffc3a5
Dateiname (*)	WorkingPaper_KT_20201129_v09.pdf
Anmerkung (*)	Projekt KT, Analyse, V0.9

(*) als Information, wird NICHT in der Blockchain gespeichert.

Zurück

Bestätigung als PDF erstellen

Dokumenten-Notarisierung - Zertifikat

Erstellt am/um 29.11.2020 - 11:04:48

Zum angegebenen Zeitpunkt wurde der Hashwert ("SHA256") eines Dokumentes sicher und unveränderbar in der Blockchain hinterlegt.

Details zum hinterlegten Dokument:

Zeitstempel	2020-11-29T11:04:48+01:00
Hashwert	07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c05166b426fae9ae
Transaktions-ID	212bf6a226764812e31f42d0733d625a43e6cd201476cf2b0ffc3a565b6e84d8
Dateiname (*)	WorkingPaper_KT_20201129_v09.pdf
Anmerkung (*)	Projekt KT, Analyse, V0.9

Die mit (*) markierten Daten wurden nicht in der Blockchain gespeichert, sie dienen nur zur Information.

Sie können den Hashwert mit folgendem QR-Code bzw. Link an das Verifikationsservice übergeben.

https://apsb01.wu.ac.at/test/?page=verify&fileHash=07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c05166b426fae9ae

Notarisierung verifizieren

Sie können hier überprüfen ob/wann ein Dokument notarisiert wurde, d.h. der digitale Fingerabdruck (Hashwert) einer Datei in der Blockchain hinterlegt wurde.

Wählen Sie dazu das entsprechende File aus (der Hashwert wird automatisch berechnet), oder geben Sie den Hashwert oder die Transaktions-ID ein.

Datei auswählen (wird NICHT auf den Server geladen), um den Hashwert zu berechnen:

Durchsuchen... Keine Datei ausgewählt.

oder Hashwert eingeben (sha256):

07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c0516

oder Transaktions-ID:

Verifizieren

Ergebnis der Verifikation

Hashwert

"07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c05166b426fae9ae" gefunden.

Es wurde ein Eintrag gefunden, d.h. das Dokument mit dem entsprechenden Hashwert wurde zum angegegeben Zeitpunkt in diesem System notarisiert.

Eintrag 1/1

Blockhash	00cab6b167c251bcbaf16e5f876864bc56406edfb8bd4971137a5b3f95b8eec1
Blockzeit	2020-11-29T11:05:08+01:00
Bestätigungen	41
Zeitstempel	2020-11-29T11:04:48+01:00
Hashwert (sha256)	07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c05166b426fae9ae
Transaktions-ID	212bf6a226764812e31f42d0733d625a43e6cd201476cf2b0ffc3a565b6e84d8

Zurück

AUSTRIA PRO

„Daten-Zertifizierung“ für die Privatwirtschaft - „Private Sector Blockchain“

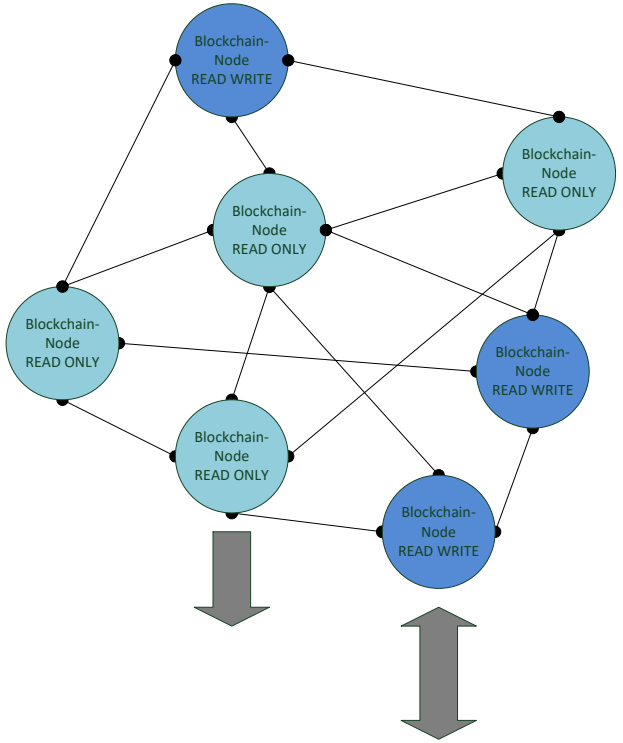
„Daten-Zertifizierung“ für die Privatwirtschaft (1/2)

- Initiative "Private Sector Blockchain"
- AUSTRIAPRO (WKO)
  - „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 (Austrian Blockchain Center) und AustriaPro (WKO)
    - Forschungsprojekt zur Klärung offener rechtlicher und organisatorischer Fragen

AUSTRIA PRO

„Daten-Zertifizierung“ für die Privatwirtschaft (2/2)

- Dieselbe technologische Basis wie APSB
  - „Schwestersystem“ => Synergien
  - Tlw. einfachere Rahmenbedingungen als im öffentlichen Bereich => Funktionale Erweiterungen je nach Anforderungen
- Blockchain-Infrastruktur
  - in Betrieb seit 2/2020
  - Dzt. ca. 10-12 Teilnehmer
- Erste Anwendungen werden demnächst im Echtbetrieb gestartet



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.
- **=> Status: Alle Themen von jeweiligen Spezialisten in Bearbeitung => Ergebnis bis Ende 2020**

AUSTRIA PRO

ABC-Research

- Private Sector Blockchain – Projektstatus 3.12.2020
- Dr. Stefan Craß

- Eigene Rechtsperson
- Parallel zu AustriaPro
- => Verein

BCI

Blockchain Initiative Austria

AUSTRIA PRO

Private Sector Blockchain - Teilnehmer

Private Sector Blockchain (Nodes)	Node Testsystem	**Node Produktivsystem**
AUSTRIAPRO	ja	**ja**
baumann.at - concepts & solutions	ja	**ja**
block42 Blockchain Company GmbH	ja	**ja**
IVM Technical Consultants 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		
Securikett Ulrich & Horn GmbH	ja	geplant
ABC Research	Vorbereitung	geplant
Nur Testsystem		
n/n (Baufirma)	ja	
n/n (IT-Development)	ja	

AUSTRIA PRO

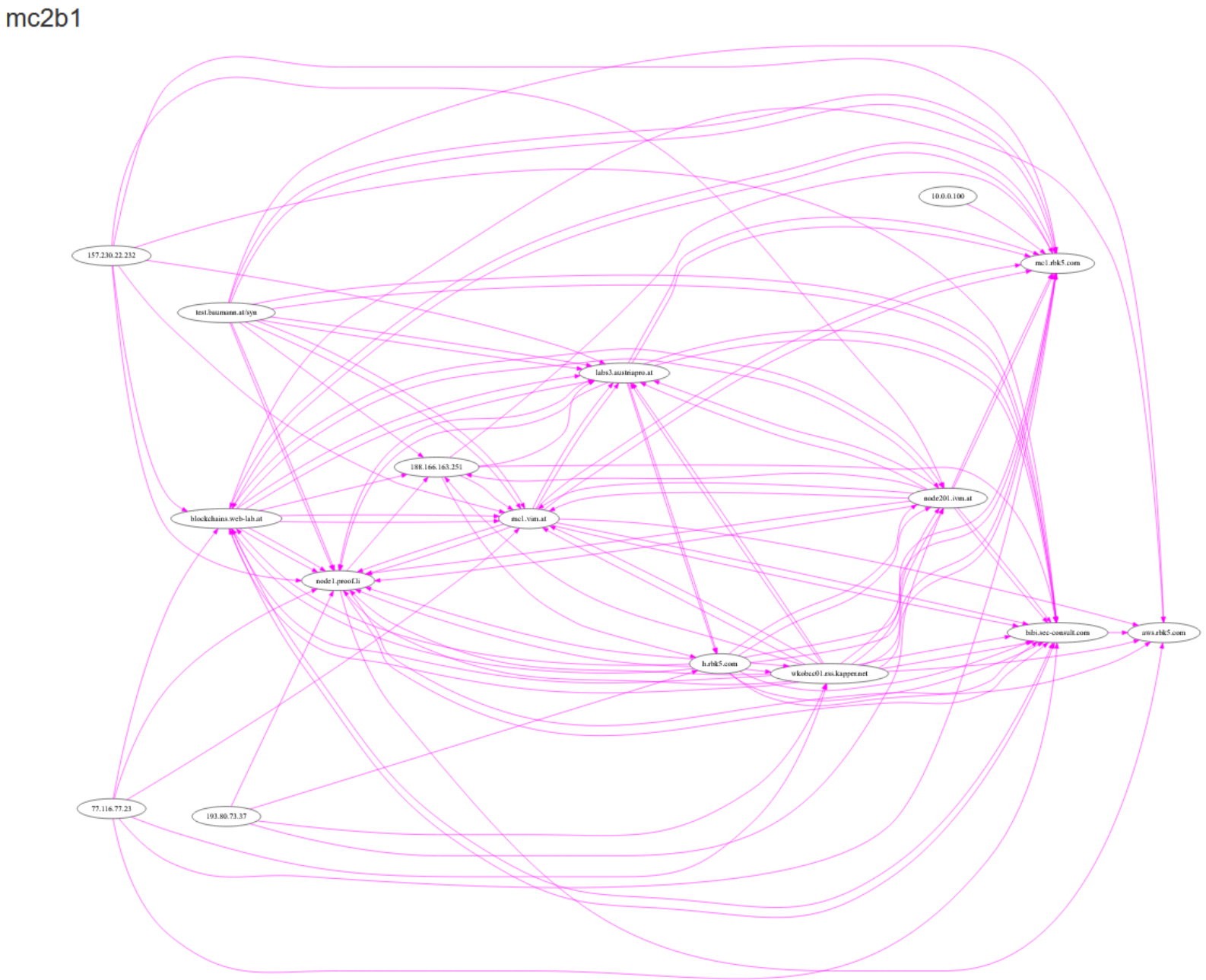
Private Sector Blockchain - Nodes

datnos-20200220

AUSTRIA PRO

AG Technik & Lab

- Status Multichain Test-Netz
- Dokumenten-ID
- Spezifikationen auf aktuellen Stand gebracht
  - Notarisierung / Daten-Zertifizierung
    - Datenstruktur im Blockchain-Stream
    - API für Applikationen (Web-GUIS und andere)
- Beispielscripts (Github) erweitert (UUID)



Multichain Test-Netz

- AustriaPro Lab
- & friends

- Offen für weitere Teilnehmer

- Diverse Beispiele (Code) verfügbar (github)

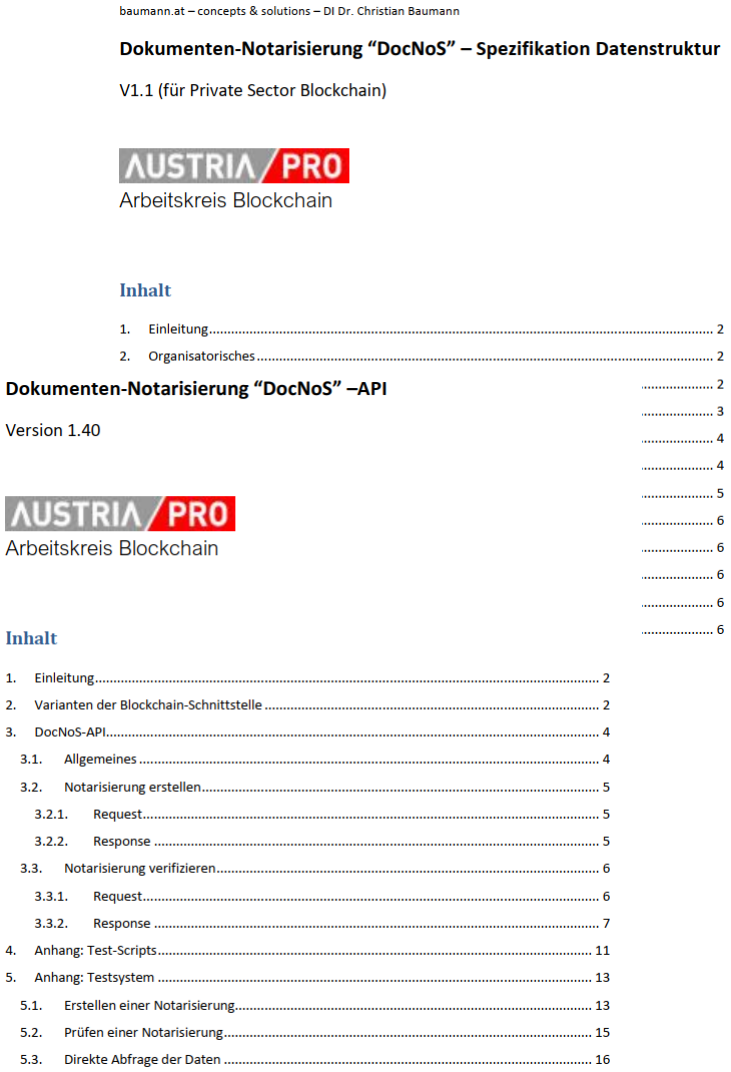
Thema Dokumenten-ID

- Anforderung: Zusatzinfo über ein Dokument (File) in Metadaten
    - Filename nicht möglich (Text …)
- Zweck
    - Dokument (firmen-)intern referenzieren (u.a. Versionen …)
    - Extern referenzieren (z.B. Zertifikat …)
    - Link zur Prüfung der Notarisierung aufbringen (VOR dem Berechnen des Hashwertes)
- Realisierung
    - Dokumenten-ID in Metadaten aufnehmen
    - „UUIDs“ („V4-GUID“), z.B. f4b99660-5a50-452e-a02f-22c86d26e6ff
    - Spezifiziert in https://tools.ietf.org/html/rfc4122
- API-Aufruf
    - Doc-Id optional, Format wird geprüft
    - API kann ebenfalls Doc-Id generieren
- Mögliche Erweiterungen
    - „Reservierung“ in der Blockchain

AUSTRIA PRO

Spezifikationen aktualisiert

- Datenstruktur in der Blockchain
  - Private Sector Blockchain V1.1
  - Public Service Blockchain – noch in Arbeit
- Rest-APIs
  - Public Service Blockchain V1.40
  - Private Sector Blockchain V1.40



baumann.at – concepts & solutions – DI Dr. Christian Baumann

Dokumenten-Notarisierung "DocNoS" – Spezifikation Datenstruktur

V1.1 (für Private Sector Blockchain)

AUSTRIA PRO
Arbeitskreis Blockchain

Inhalt

Dokumenten-Notarisierung "DocNoS" –API ... 2

... 3

Version 1.40 ... 4

... 4

... 5

AUSTRIA PRO
Arbeitskreis Blockchain ... 6

... 6

... 6

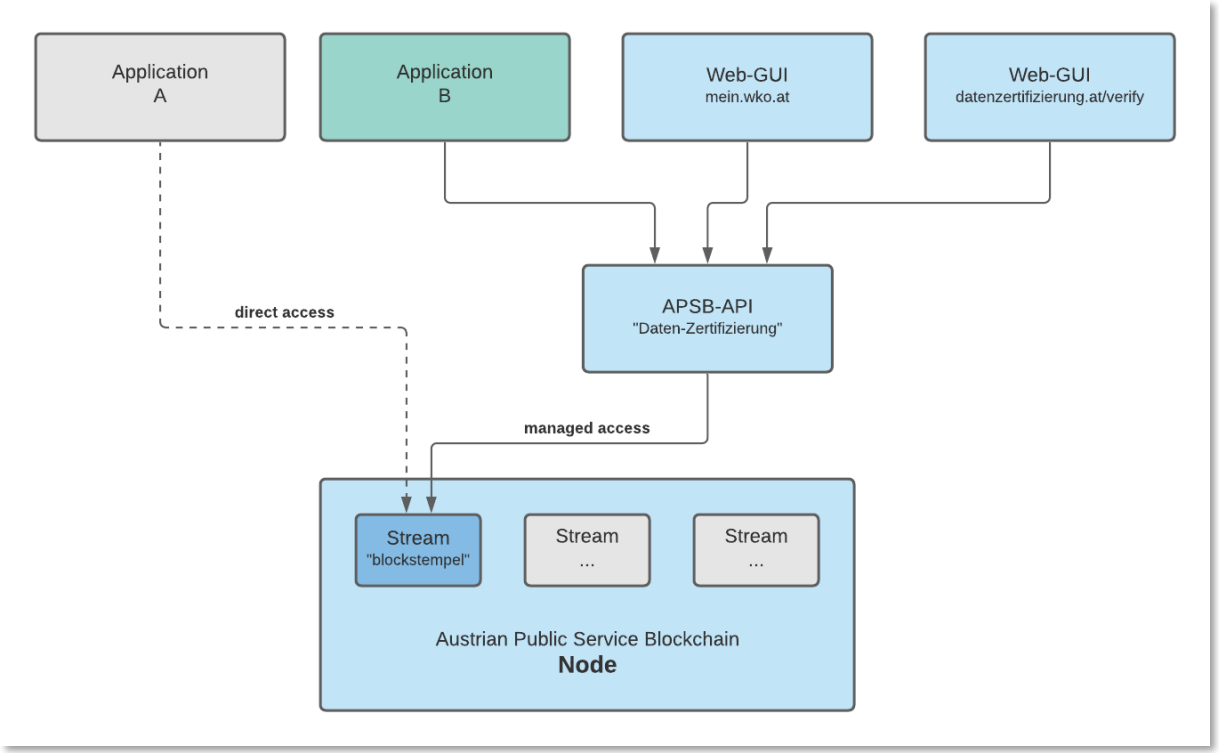
... 6

... 6

Inhalt

AUSTRIA PRO

Varianten der Blockchain-Schnittstelle



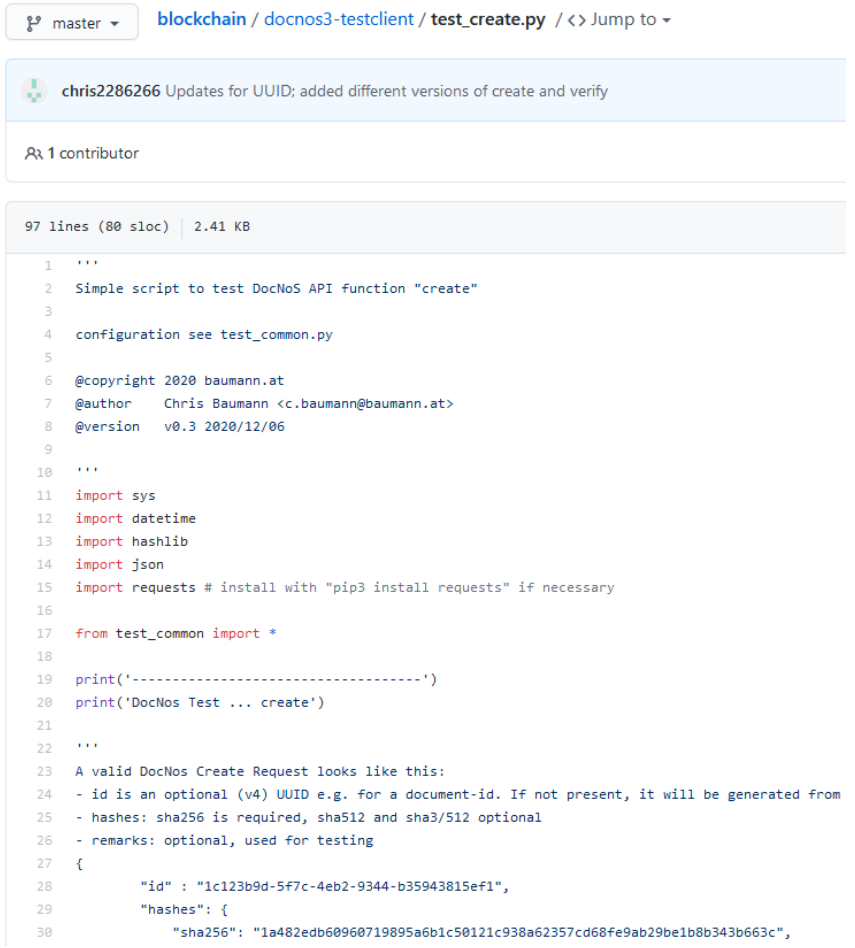
- Direkter Zugriff von der Anwendung auf den Blockchain-Node (per Multichain-RPC-API)
- Zugriff über das API
  - geringere Komplexität
  - mehrere Anwendungen
  - Zugriffsberechtigungen

AUSTRIA PRO

Neue Beispielscripts auf GitHub

- API „Daten-Zertifizierung“ aufrufen
- Typen
  - APSB – „Blockstempel-V2“ Format
  - Private Sector BC – „standard“ Format
- Funktionen
  - Create … Hashwert/e hinterlegen
  - Verify … Nach Hashwerten/Tx-ID suchen
  - NEU (12/2020) Integration der Dokumenten-ID (UUID)
    - Create: Übergeben oder autom. Generieren im API
    - Verify: Als Suchparameter
- Sourecode in Python

- https://github.com/austriapro/blockchain/tree/master/docnos3-testclient



open space

- open space – Projekte, Initiativen, Informationen
  - „Gretchenfrage: Wie vertrauenswürdig ist Blockchain-Technologie?“, Klaus Veselko, cis-cert
  - “Status Blockchain Trade Platform (BTP)“, Andreas Luxbauer & Ergun Türker
  - 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