

Arbeitskreis Blockchain

Allgemeines & Arbeitsgruppe Technik & Blockchain Lab

Dr. Christian Baumann

1.10.2020



Inhalt

- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab
- open space - Projekte, Initiativen, Informationen
 - Nuran Babadostu - „Blockchain Trade Platform BTP“
 - weitere Meldungen (spontan)
 - Zoltan Fazekas - „Bloxberg“ (angefragt)

Austrian Public Service Blockchain („APSB“)

- 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 (zugesagt)
 - **WU Wien - Blockchain-Node in Betrieb - Anwendung demnächst**
 - Kontrollbank (zugesagt)
- Weitere (angefragt)
 - FH St. Pölten, TU Wien ...

Austrian Public Sector Blockchain - Aktuelle Teilnehmer

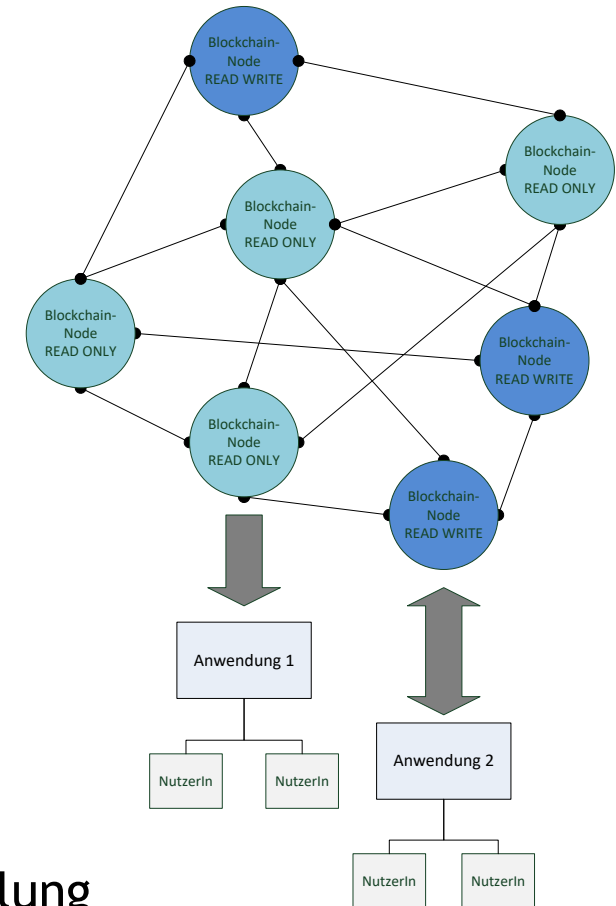
Austrian Public Sector Blockchain (Nodes)	Node Test	Node Produktiv
BRZ (Bundesrechenzentrum)	ja (2)	ja (2)
Stadt Wien - MA01	ja (2)	ja
WKO (Wirtschaftskammer Österreich)	ja	ja
nic.at/cert.at	ja	ja
WU (Wirtschaftsuniversität Wien)	ja	ja
AUSTRIAPRO	(ja)	

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 ...

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



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
 - zukünftig ev. „Dual-Verify“ - auch Dokumente der Private-Sector Blockchain

Überprüfen einer Datenzertifizierung

Der digitale Fingerabdruck (Hashwert) des Dokumentes kann neu errechnet werden. Dazu wählen Sie das Dokument erneut aus. Die entsprechenden Daten werden dann in der Blockchain gesucht und angezeigt. Sie können die Überprüfung aber auch durch Eingabe der Transaktions-ID oder des digitalen Fingerabdrucks (Hashwert) der Daten durchführen.

Wenn das gleiche Dokument mehrfach eingetragen wurde, ist der älteste Eintrag der relevanteste.

Dokument auswählen

Keine Datei ausgewählt.

Digitaler Fingerabdruck (Hashwert sha256)

oder Transaktions-ID

Ergebnis der Verifikation



Hashwert "2a1bea43d639b437dbf05ad72189238a5101246f18651fdc41e37d90b81eb592" gefunden.

Eintrag 1/1

Blockhash	0048cf0bd3cb48b71da64a45830fd02035972d2f23cdcc37cd33805a7da6f968
Blockzeit	2019-12-17T07:01:28+01:00
Bestätigungen	1508
Zeitstempel	2019-12-17T07:01:15+01:00

WKO weitere Usecases

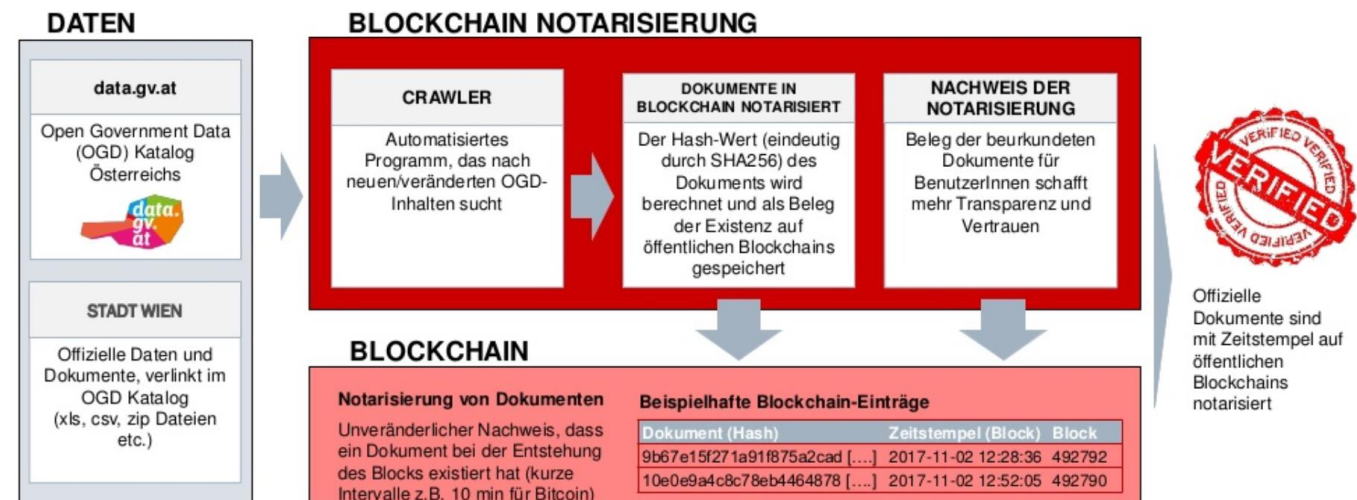
- In Kooperation mit WIFI
 - Daten-Zertifizierung für elektronische Dokumente
 - Personenzertifikate und diverse andere
 - Automatisierte Erstellung
 - Inhalte von Personenzertifikaten
 - Vgl. AustriaPro Projekt 2019
 - Freiwillig!
 - Gemäß DSGVO
 - Vgl. Gutachten Prof. Forgo
 - „Ausgewählte datenschutzrechtliche Fragen im Zusammenhang mit der Personenzertifizierung in der Blockchain“
 - <https://www.wko.at/service/netzwerke/blockchain-gutachten-studien-publikationen.html>
 - Ggf. Klärung offener Fragen in ABC Forschungsprojekt



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



APSB - WU (Wirtschaftsuniversität Wien)

- Neuer Teilnehmer per 9/2020
- Blockchain-Knoten läuft, Applikation wird soeben installiert
- Use-Case
 - Notarisierung („Daten-Zertifizierung“)
 - Phase 1:
 - Wissenschaftliche MitarbeiterInnen und StudentInnen
 - Publikationen, Diplomarbeiten, Dissertationen ...
 - Phase 2: ?
 - Details
 - 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 ...

APSB - WU - Notarisierung



Erstellen Verifizieren

Notarisierung erstellen - TEST-WU

Aenean mattis venenatis sapien, in facilisis diam tincidunt vel. Ut volutpat purus leo ut nulla.

Datei auswählen (wird NICHT auf den Server geladen):

Durchsuchen... Test-Dokument_042.docx

Berechneter Hashwert (sha256):

13190e7e845a4740cf2b886bae6ed130bf3295a12f7beb05b882f1a8eafe2250

Dateiname (*):

Test-Dokument_042.docx

Anmerkung (optional, *):

Testing by CB

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

Erstellen

Praesent sodales fringilla vulputate. Vivamus nec commodo sapien. Vest vitae diam id nisi commodo blandit sit amet sit amet justo.

[Bestätigung als PDF erstellen](#)



Datenzertifizierung - Bestätigung

Erstellt am/um 30.09.2020 - 11:28:29

Zum angegebenen Zeitpunkt wurde der Hashwert ("SHA256") unveränderbar in der Blockchain hinterlegt.

Details zum hinterlegten Dokument:

Zeitstempel	2020-09-30T11:28:29+02:00
Hashwert	13190e7e845a4740cf2b886bae6ed130bf3295a12f7beb05b882f1a8eafe2250
Transaktions-ID	7a45be9c0b1c86ba0b7da728534c0250fc70f43ecbd3d2ca1444584a5c1b4e28
Dateiname (*)	Test-Dokument_042.docx
Anmerkung (*)	Testing by CB

Die mit (*) markierten Daten wurden nicht in der Blockchain gespeichert.

Sie können die Transaktions-ID mit folgendem QR-Code bzw. übergeben.



Erstellen Verifizieren

Ergebnis der Verifikation - TEST-WU



Hashwert "13190e7e845a4740cf2b886bae6ed130bf3295a12f7beb05b882f1a8eafe2250" gefunden.

Eintrag 1/1

Blockhash	0068b3cebd6272b87141e8873eeea6c4c52f9ecdb77a6dcfe7be7ae3db845ab27
Blockzeit	2020-09-30T11:28:46+02:00
Bestätigungen	9
Zeitstempel	2020-09-30T11:28:29+02:00
Hashwert (sha256)	13190e7e845a4740cf2b886bae6ed130bf3295a12f7beb05b882f1a8eafe2250
Transaktions-ID	7a45be9c0b1c86ba0b7da728534c0250fc70f43ecbd3d2ca1444584a5c1b4e28

Zurück

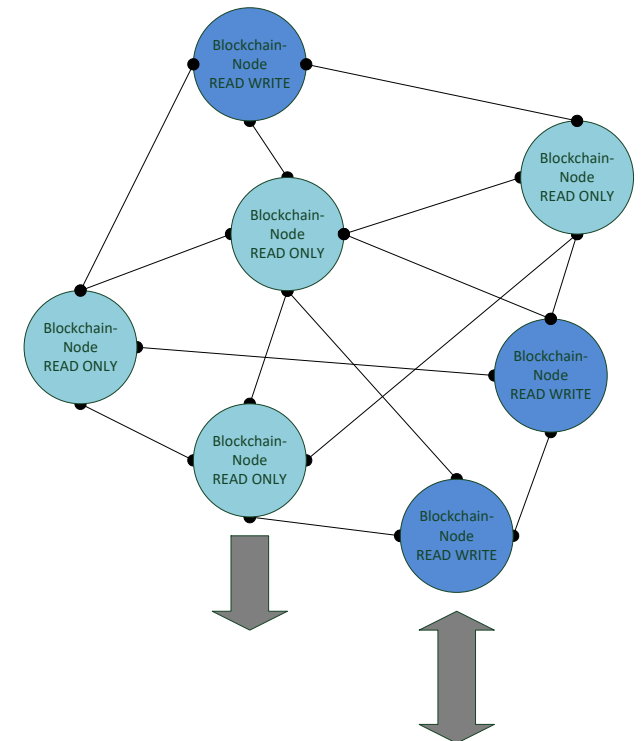
„Daten-Zertifizierung“ für die Privatwirtschaft - „Private Sector Blockchain“

„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

„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



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.

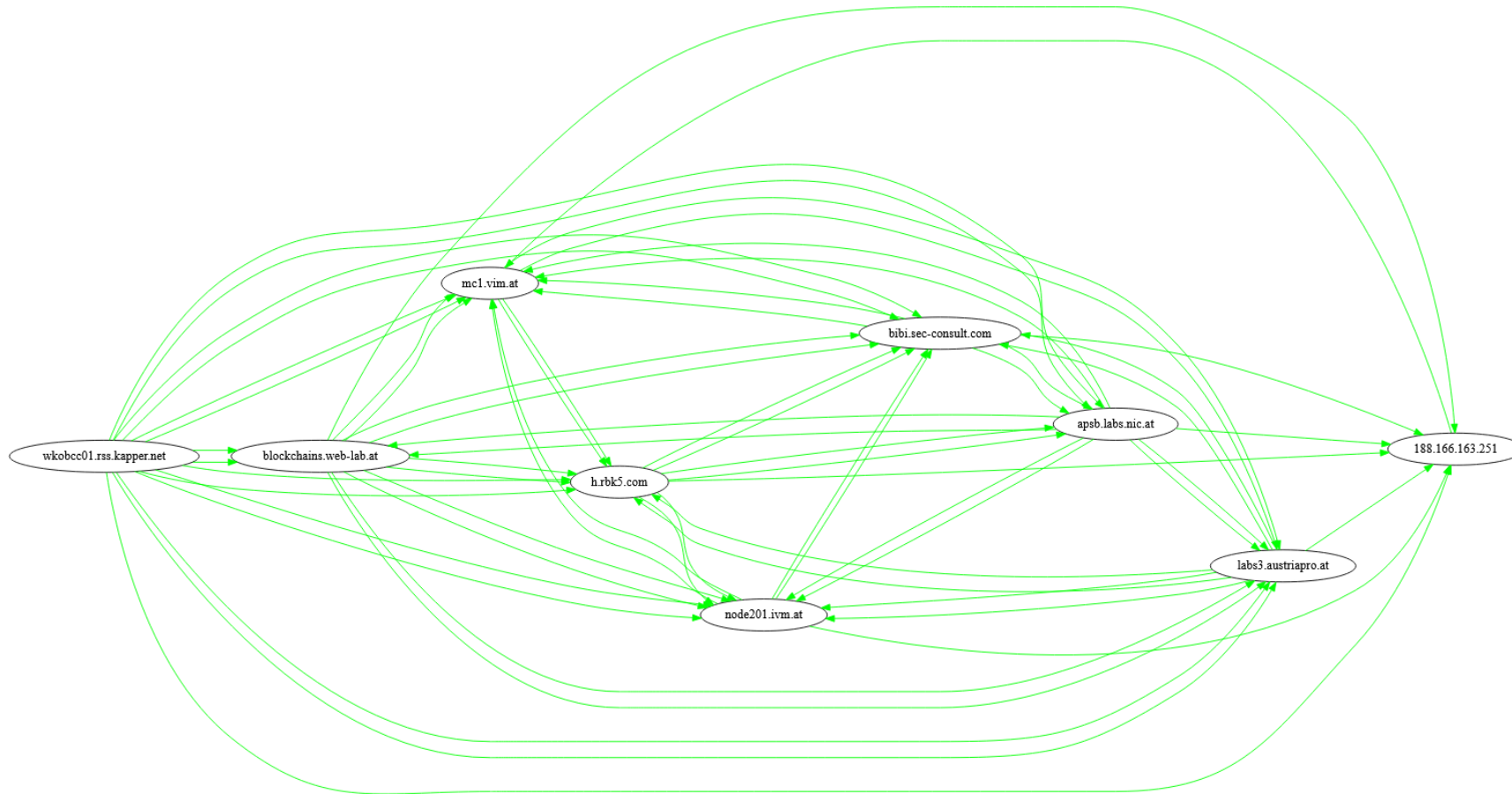
- Welche Besonderheiten sind zu beachten, damit eine solche Blockchain-Infrastruktur nicht in Konflikt mit den Anforderungen der **DSGVO** kommen kann? (Können Hashwerte personenbezogene Daten sein und wenn ja, welche Konsequenz hat das?)
- Wie kann die **Governance** gestaltet sein, damit ein solches 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**

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	

Private Sector Blockchain - Nodes

datnos-20200220



"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>

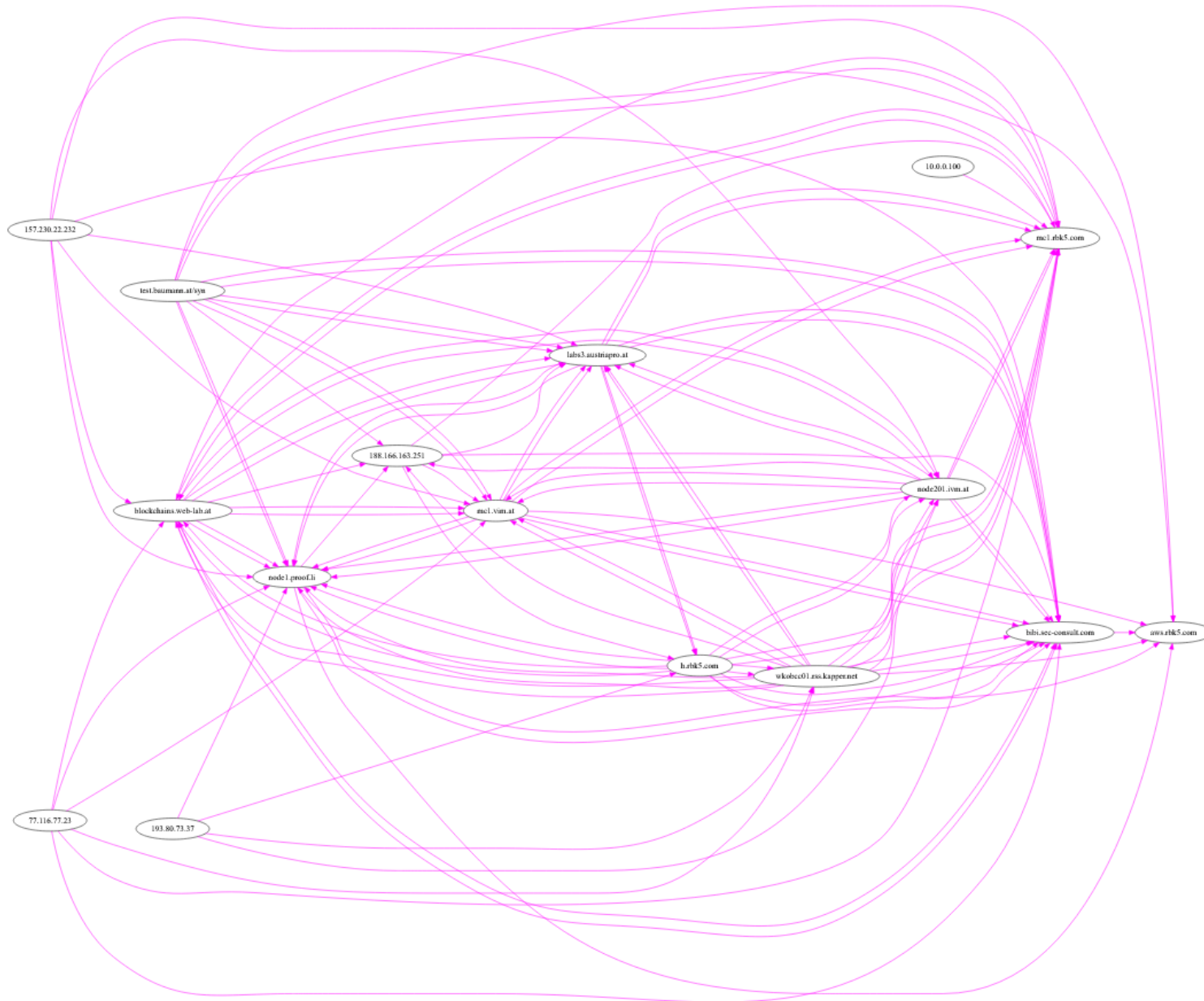
Zusammenfassung:

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.

AG Technik & Lab

- Status Multichain Test-Netz
- Neues Beispielscript
- European Blockchain Service Infrastructure

mc2b1



Multichain Test-Netz

- AustriaPro Lab
- & friends
- Offen für weitere Teilnehmer
- Diverse Beispiele (Code) verfügbar (github)

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
- Sourecode in Python

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

```
cb1 blockchain / docnos3-testclient / test_create.py / <> Jump to  
chris2286266 First release ...  
1 contributor  
75 lines (60 sloc) | 1.91 KB  
1 ...  
2 Simple script to test DocNoS API function "create"  
3  
4 configuration see test_common.py  
5  
6 @copyright 2020 baumann.at  
7 @author Chris Baumann <c.baumann@baumann.at>  
8 @version v0.2 2020/09/30  
9  
10 ...  
11 import sys  
12 import datetime  
13 import hashlib  
14 import json  
15 import requests # install with "pip3 install requests" if necessary  
16  
17 from test_common import *  
18  
19 print('-----')  
20 print('DocNos Test ... create')  
21  
22 ...  
23 A valid DocNos Create Request looks like this: (sha256 is required, sha512 and sha3/512 optional)  
24 {  
25     "hashes": {  
26         "sha256": "1a482edb60960719895a6b1c50121c938a62357cd68fe9ab29be1b8b343b663c",  
27         "sha512": "294a725daacea98a340ce946182105e12448e7c1147424f94a0eb453eb51373a39f0e563d828aea092e",  
28         "sha3/512": "f210c7bc0c281b844a989160186eb0f8a1ac2a996cd3d6db8e0b4074015e3521b50dcabd2ac597c71",  
29     },  
30     "remarks": "optional remarks"  
31 }
```

European Blockchain Services Infrastructure

- Kurzbeschreibung
- Usecases im Test
 - Self Sovereign Identity
 - Verifiable Credentials
 - ...
- Zeithorizont
- Node betreiben?

- Status / Vergleich zu APSB
- Konnex zu AustriaPro?











EBSI

European Blockchain Services Infrastructure

AUSTRIA / PRO

EU hat mehrere (digitale) „Building Blocks“

The screenshot shows the website <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>. The header includes the CEF Digital Connecting Europe logo, navigation tabs for 'About us', 'Building Blocks', and 'DSIs', a 'CONTACT US' button, and a search icon. The main content area features a grid of digital building blocks, each with an icon, a title, and a brief description. A yellow 'APPLY FOR GRANTS' button is located at the bottom right of the grid.

 Big Data Test Infrastructure A free big data analytics sandbox to power your data-driven decision-making	 Blockchain (EBSI) Build the next generation of European Blockchain Services Infrastructure	 Context Broker Make data-driven decisions in real time, at the right time
 eArchiving Preserve, migrate and reuse data securely, according to European Standards	 eDelivery Exchange electronic data and documents in an interoperable and secure way	 eID Offer services capable of electronically identifying users from all across Europe
 eInvoicing Send and receive electronic invoices in line with European directives	 eSignature Create and verify electronic, paperless signatures	 eTranslation Enable multilingual public services and communication
 Once Only Principle Reduce administrative burden for individuals and businesses		APPLY FOR GRANTS

... einer davon die Blockchain ...



Introducing the European Blockchain Services Infrastructure (EBSI)

Blockchain technology has enormous potential to enhance the way that citizens, governments and businesses interact, by enhancing trust between entities and improving the efficiency of operations.

The European Blockchain Services Infrastructure (EBSI) is a joint initiative from the European Commission and the [European Blockchain Partnership](#) (EBP) to deliver EU-wide cross-border public services using blockchain technology. The EBSI will be materialised as a network of distributed nodes across Europe (the blockchain), leveraging an

increasing number of applications focused on specific use cases. In 2020, EBSI will become a [CEF Building Block](#), providing reusable software, specifications and services to support adoption by EU institutions and European public administrations.

EBSI Projekt seit 2019

EBSI Key Figures

€4M/year

Budget invested
2019-2020

4

Use cases selected
in 2019

300+

Contributors
and counting

20

MS hosting at least one node

27

nodes live

10

nodes in setup phase

Use cases in Test (2019/2020)



Notarisation

Leveraging the power of blockchain to create trusted digital audit trails, automate compliance checks in time-sensitive processes and prove data integrity.



Diplomas

Giving control back to citizens when managing their education credentials; significantly reducing verification costs and improving authenticity trust.



European Self-Sovereign Identity

Implementing a generic Self-Sovereign Identity capability, allowing users to create and control their own identity across borders without relying on centralised authorities.

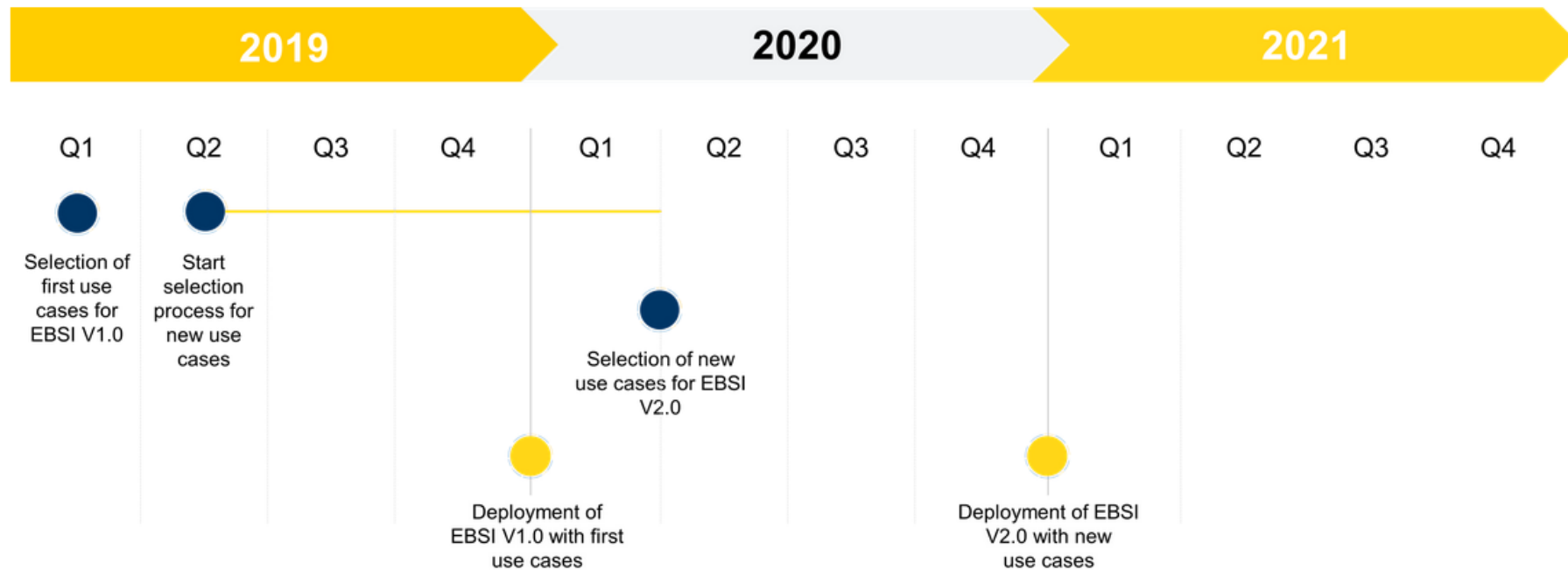


Trusted Data Sharing

Leveraging blockchain technology to securely share data (e.g. IOSS VAT identification numbers and import one-stop-shop) amongst customs and tax authorities in the EU.

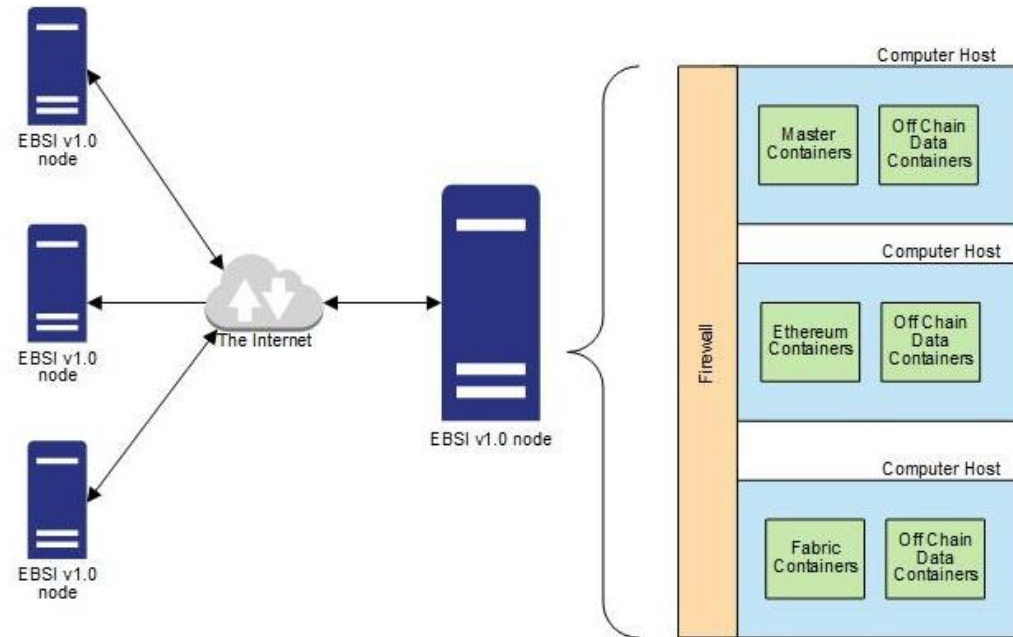
Zeithorizont ...

What milestones
are paving the way towards EBSI?



Node betreiben ...

- 3 Hosts mit ca. 14 Services ...



<https://ec.europa.eu/ebsi/>

r+Hostir

BESU	EBSI Nodes (All)	MS EBSI Node	TCP 48745	Ethereum (Besu) ledger (RPC Service)
BESU	EBSI Nodes (All)	MS EBSI Node	TCP+UDP 48733	Ethereum (Besu) ledger (Syncro Service)
Master/Application	EBSI Nodes (All)	MS EBSI Node	TCP + UDP 24007, 24008 & TCP 49152	GlusterFS (not used in V1.0)
Master/Application, BESU, FABRIC	EBSI Nodes (All)	MS EBSI Node	TCP 27017	Mongo DB (Redundancy Option) (not used in V1.0)
Master/Application, BESU, FABRIC	MS management network OR internet	MS EBSI Node	TCP 48790	Cockpit
FABRIC	EBSI Nodes (All)	MS EBSI Node	TCP 7054	Fabric CA Service
FABRIC	EBSI Nodes (All)	MS EBSI Node	TCP 7053	Fabric Peer External (Even Notification)
FABRIC	EBSI Nodes (All)	MS EBSI Node	TCP 7051	Fabric Peer Internal (GRPC)
FABRIC	EBSI Nodes (All)	MS EBSI Node	TCP 7050	Fabric Orderer Service
FABRIC	Internet	MS EBSI Node	TCP 48780	Fabric Block Explorer
Master/Application	EBSI Nodes (All)	MS EBSI Node	TCP 7000	Cassandra DB
Master/Application, BESU, FABRIC	Internet	MS EBSI Node	TCP 443	NGINX (HTTPS Traffic)
Master/Application, BESU, FABRIC	MS management network OR Internet	MS EBSI Node	TCP 48722	SSH (for Node Computer Unit admin)
Master/Application, BESU, FABRIC	infra.ebsi.xyz	MS EBSI Node	TCP 8140	For configuration management


An „functional test“ teilnehmen ...

- EU Account anlegen
- Für EBSI Test freischalten lassen
- User Journey testen
 - Wallet anlegen
 - DID wird generiert
 - Verifiable Credentials anfordern
 - Z.B. eID
 - Universitäts-Diplom ...
 - Dokumente Notarisieren ...


Disclaimer: this is a demo website to show the technical capabilities of the EBSI project. We are using dummy data. All the public entities are simulated, there is no real interaction with any of them.

Test EBSI User Journey Demo by taking the following steps in order.


European Self-Sovereign Identity (SSID)

 **Create your EBSI Wallet account**
Open the EBSI Wallet and authenticate via your EU Login, then setup your EBSI account to follow the user journey. In your wallet, you will create your own Decentralised ID and a set of public-private keys. [Wallet](#)

ESSIF Sample App: Issue eID Verifiable Credential

 **Get your eID Verifiable Credential**
Open a request on the Sample Verifiable ID Issuer website to receive your verifiable ID. The Sample Verifiable ID Issuer verifies the request and issues the ID Verifiable Credential, which will be stored in your wallet. With your digital ID, you will have access to other services on the EBSI platform. [eID Verifiable Credential](#)

Diploma Sample App: Issue Bachelor's Diploma

 **Get your Bachelor's Diploma**
Open the Sample University - Bachelor's Programme website and make a request to get your Bachelor's Diploma. The Sample University - Bachelor's Programme verifies your request and your Verifiable eID and then issues the Bachelor's Diploma Verifiable Attestation, which will be stored in your wallet. [Bachelor's Diploma](#)

Status / Vergleich

- EBSI
 - „Eierlegende Wollmilchsau“ => technisch, organisatorisch ... extrem komplex, aufwändig, kosten- & zeitintensiv
- Vergleich mit APSB?
 - Schwer!
 - Technischer Aufwand EBSI (Nodes, Implementierungen ...) min. Faktor 10 komplexer
 - APSB Infrastruktur und erster Usecase seit Ende 2019 in Echtbetrieb
- EBSI: „Top-Down“ / APSB: „Bottom-Up“

Konnex zu AustriaPro?

- Weitere Beobachtung des Projektes
 - U.a. im Rahmen der AG Technik & Lab
- Definition next steps nach Vorliegen von EBSI V2.0
 - Ca. Q1/2021
 - Mögliche Koppelung APSB zu EBSI (z.B. in Form von Anchoring)
 - Ggf. Node betreiben und Umsetzung von Usecases überlegen
 - Abhängig von Finanzierung

open space

- open space - Projekte, Initiativen, Informationen
 - Zoltan Fazekas - „Bloxberg“
 - Nuran Babadostu - „Blockchain Trade Platform BTP“
 - 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

AUSTRIA / PRO