Arbeitskreis Blockchain

Allgemeines & Arbeitsgruppe Technik & Blockchain Lab

Dr. Christian Baumann

1.10.2020

AUSTRIA PRO

Inhalt

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

AUSTRIA PRO

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 …

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

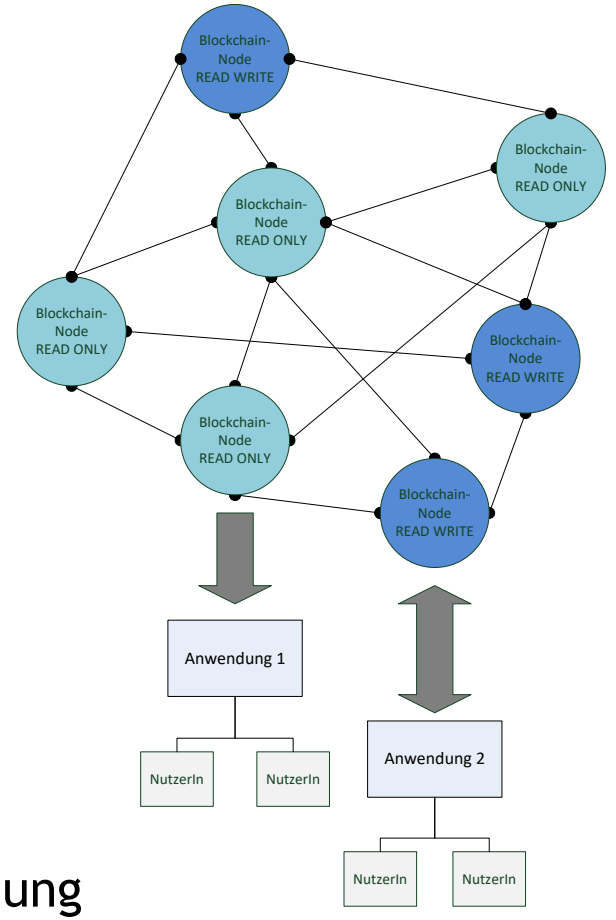
Austrian Public Service Blockchain (APSB) Vereinbarung

- **„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

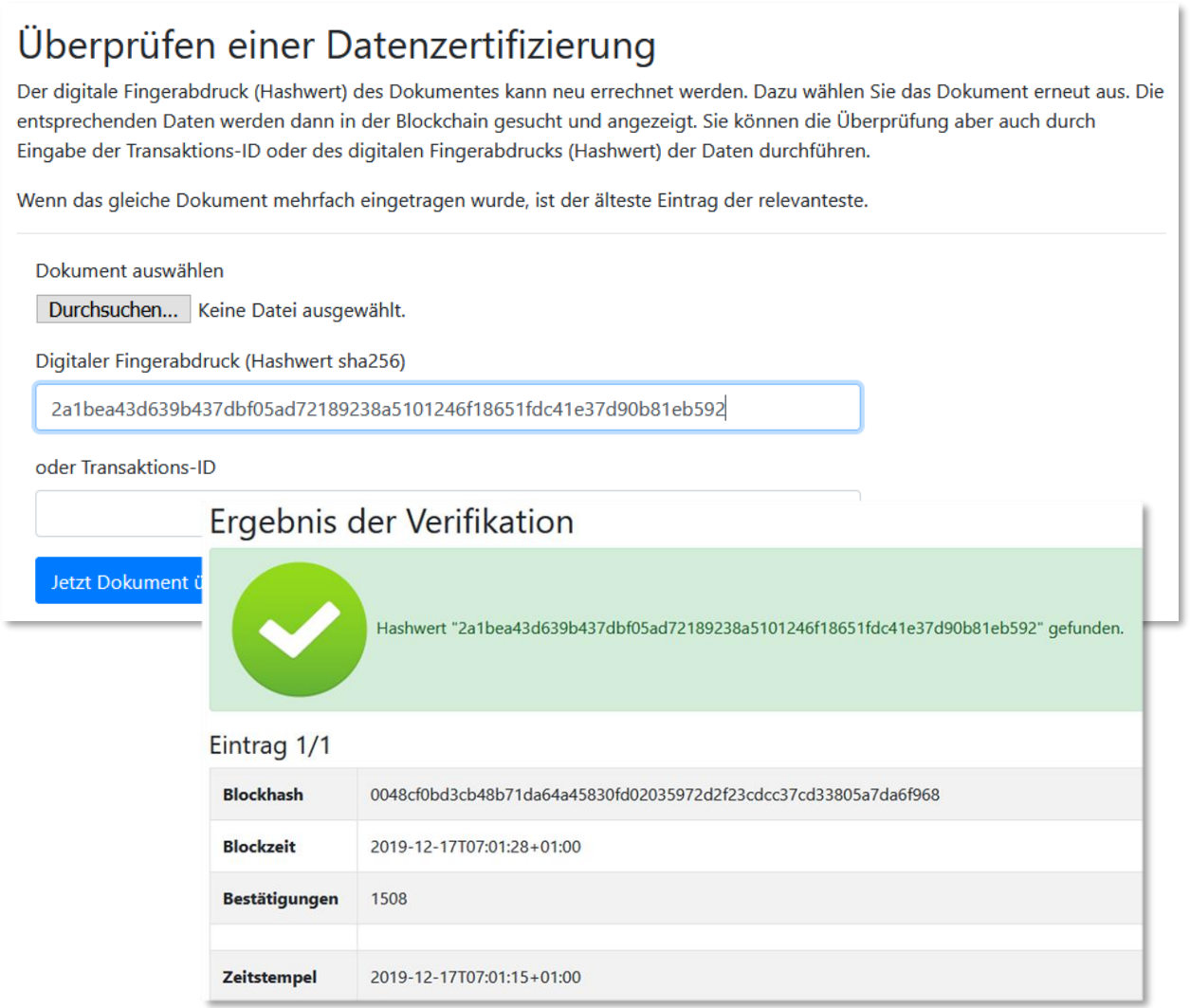
- Inhalt
  - Gegenstand und Zweck
  - Architektur
  - Begriffsbestimmungen
  - Beitritt zur APSB
  - Rechte und Pflichten von Anwendungsverantwortlichen
  - Rechte und Pflichten der Knotenverantwortlichen
  - Technische und organisatorische Vorkehrungen
  - Haftungsregelungen
  - Entzug der Teilnahme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



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



WKO weitere Usecases

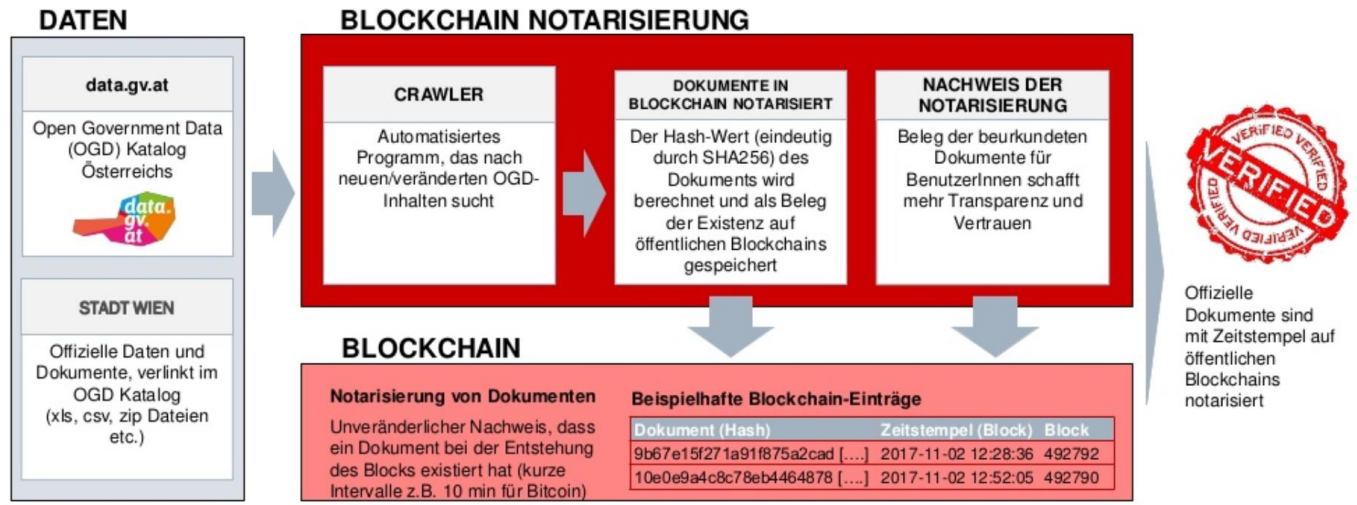
- In Kooperation mit WIFI
  - Daten-Zertifizierung für elektronische Dokumente
    - Personenzertifikate und diverse andere
    - Automatisierte Erstellung
  - Inhalte von Personenzertifikaten
    - Vgl. AustriaPro Projekt 2019
    - Freiwillig!
    - Gemäß DSGVO
      - Vgl. Gutachten Prof. Forgo
        - „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

AUSTRIA PRO

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



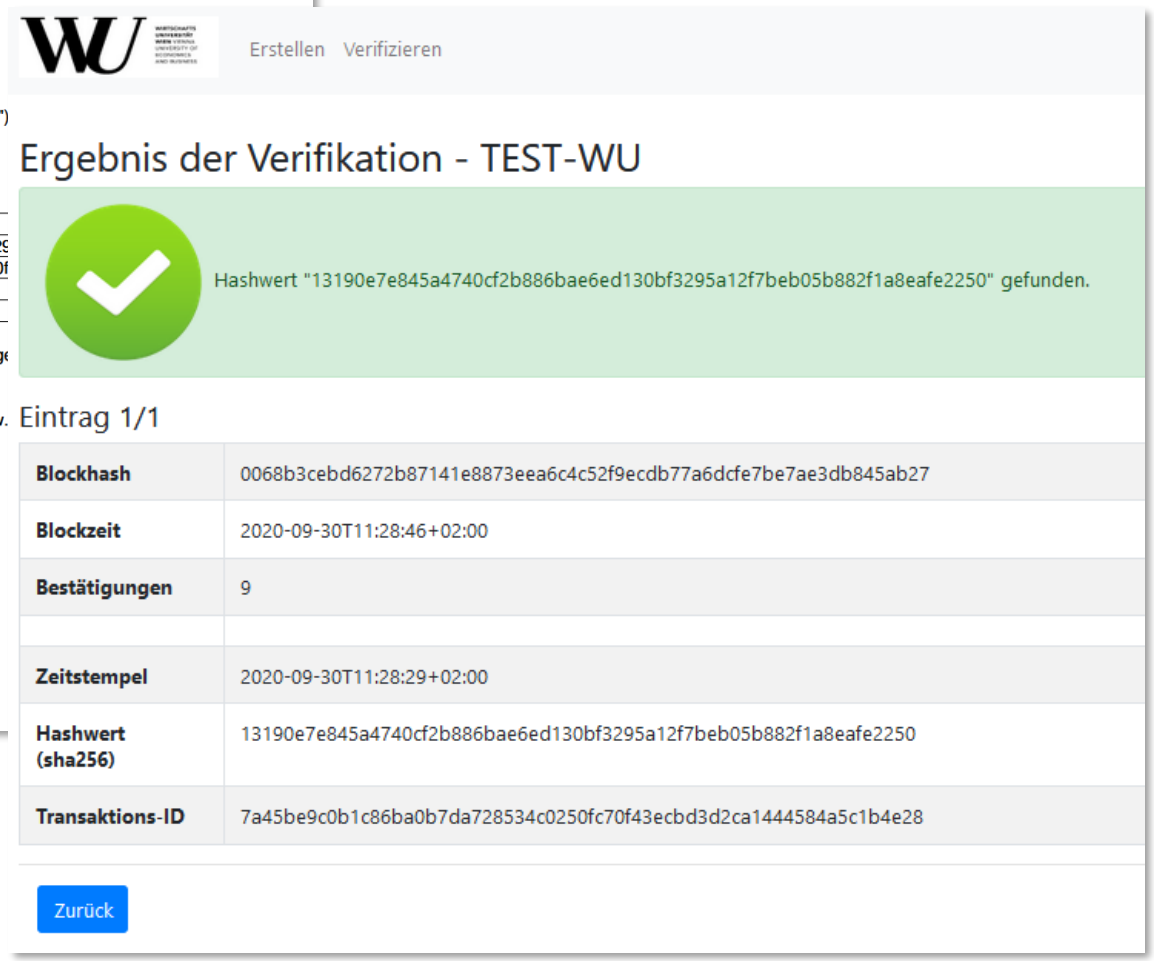
https://www.slideshare.net/DigitalesWien/1-blockchainpilot-der-stadt-wien-ogd-notarization

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 …

AUSTRIA PRO

APSB – WU - Notarisierung



AUSTRIA PRO

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

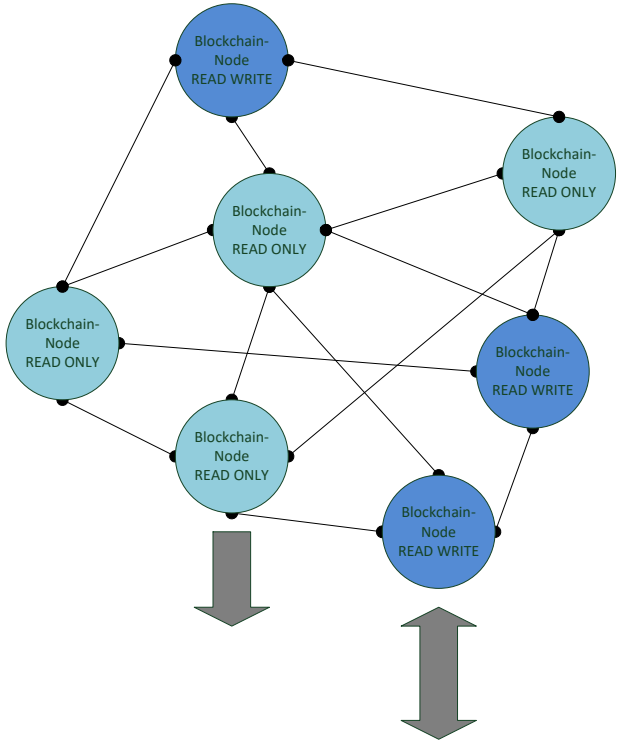
„Daten-Zertifizierung“ für die Privatwirtschaft (1/2)

- 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

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

"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:

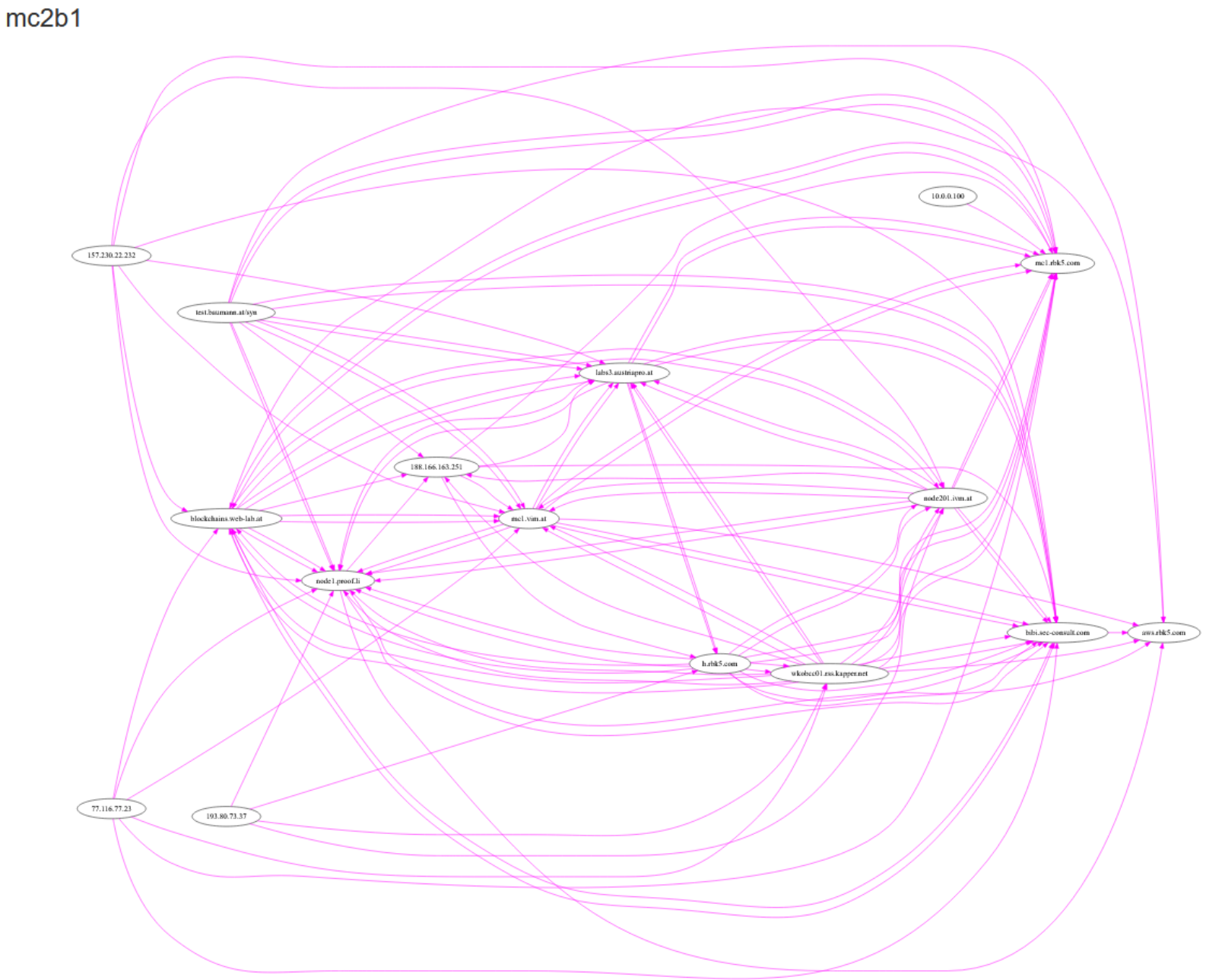
Es ist daher von einer verlässlichen Möglichkeit, zu beweisen, dass elektronische Daten zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert haben und seither nicht verändert wurden, auszugehen.

AUSTRIA PRO

AG Technik & Lab

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

AUSTRIA PRO



Multichain Test-Netz

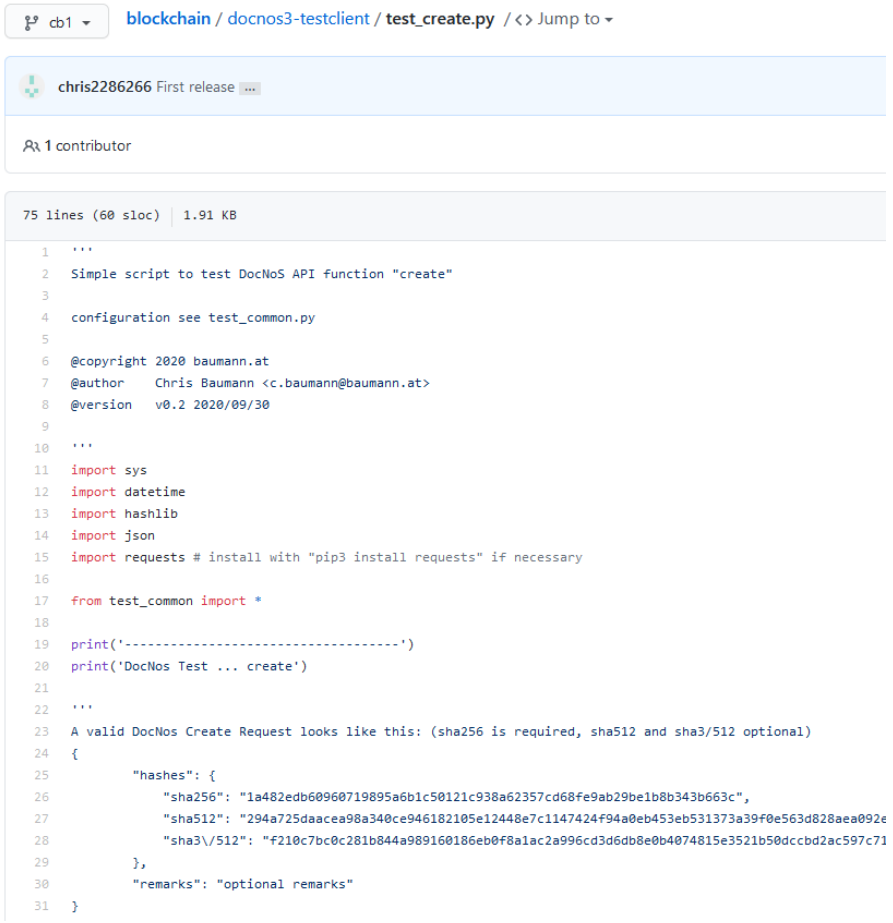
- AustriaPro Lab
- & friends

- 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

AUSTRIA PRO

European Blockchain Services Infrastructure

- Kurzbeschreibung
- Usecases im Test
  - Self Sovereign Identity
  - Verifyable Credentials
  - …
- Zeithorizont
- Node betreiben?

- Status / Vergleich zu APSB
- Konnex zu AustriaPro?

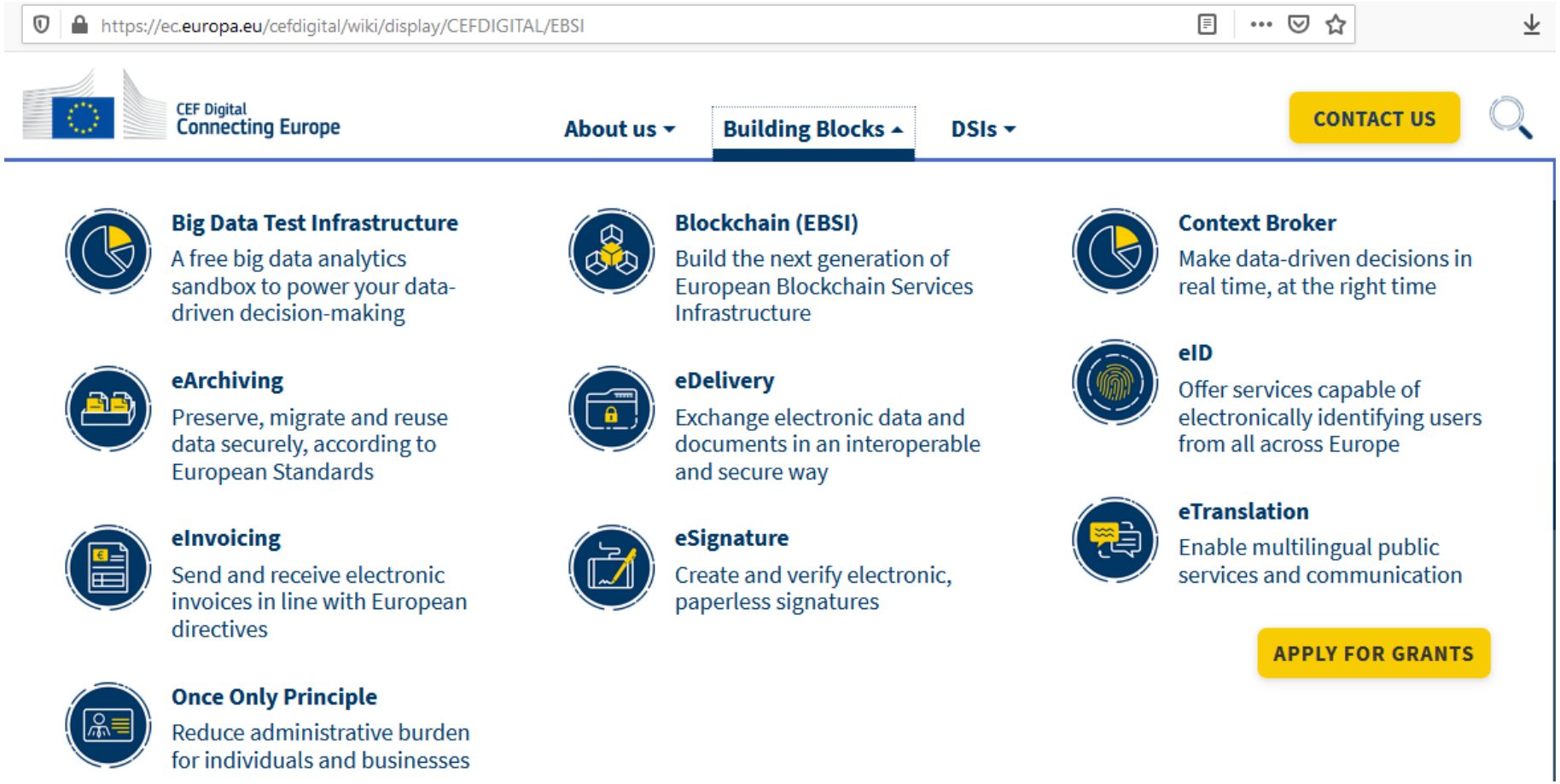
AUSTRIA PRO

EBSI

European Blockchain Services Infrastructure

AUSTRIA PRO

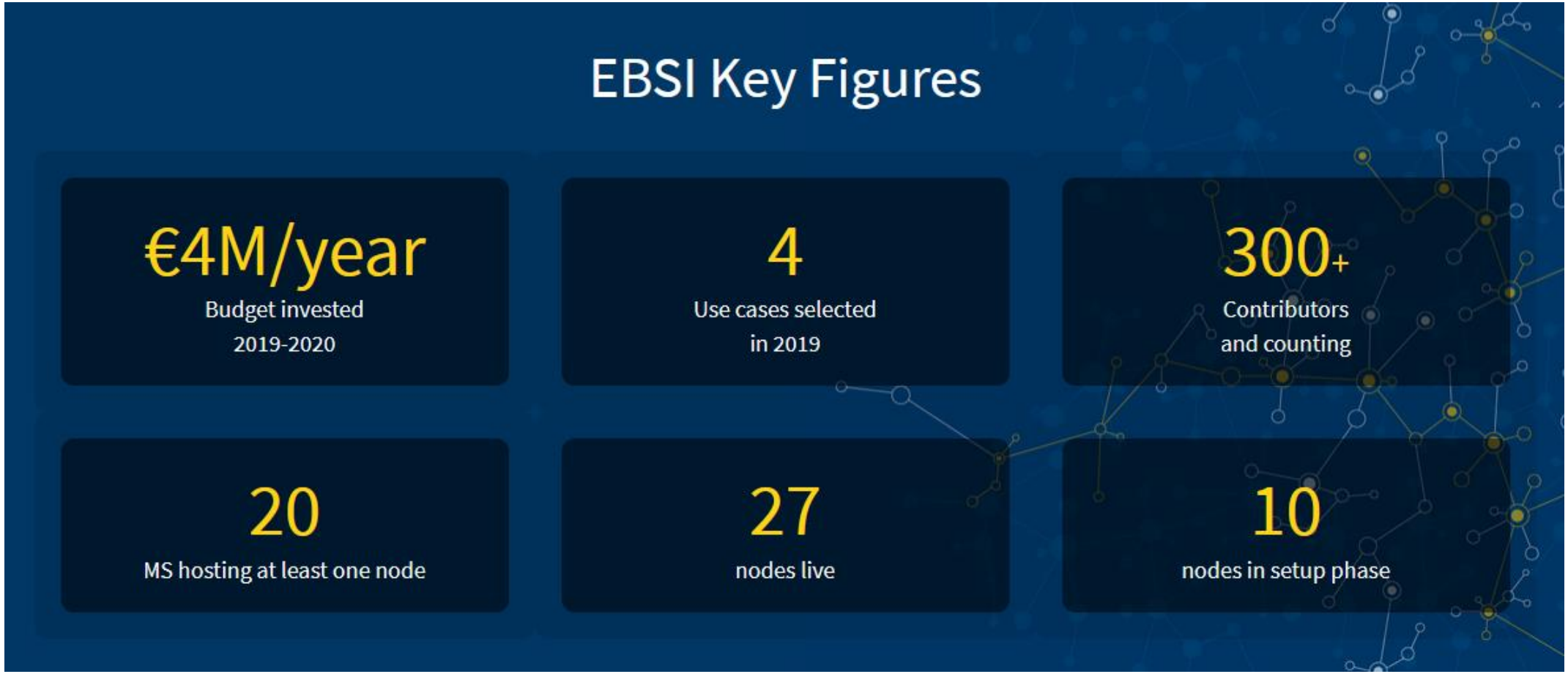
EU hat mehrere (digitale) „Building Blocks“



AUSTRIA PRO

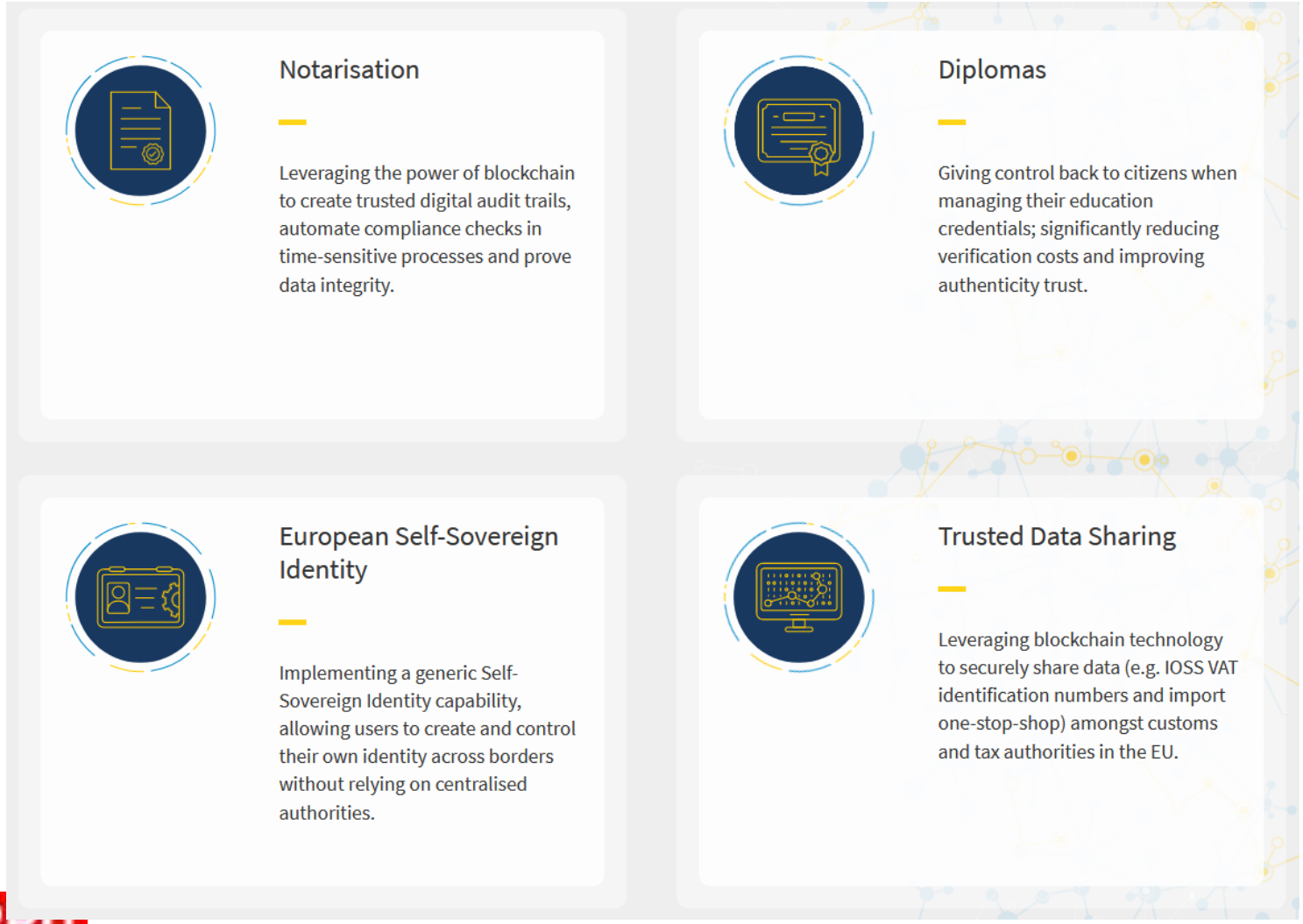
… einer davon die Blockchain …

EBSI Projekt seit 2019



AUSTRIA PRO

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.

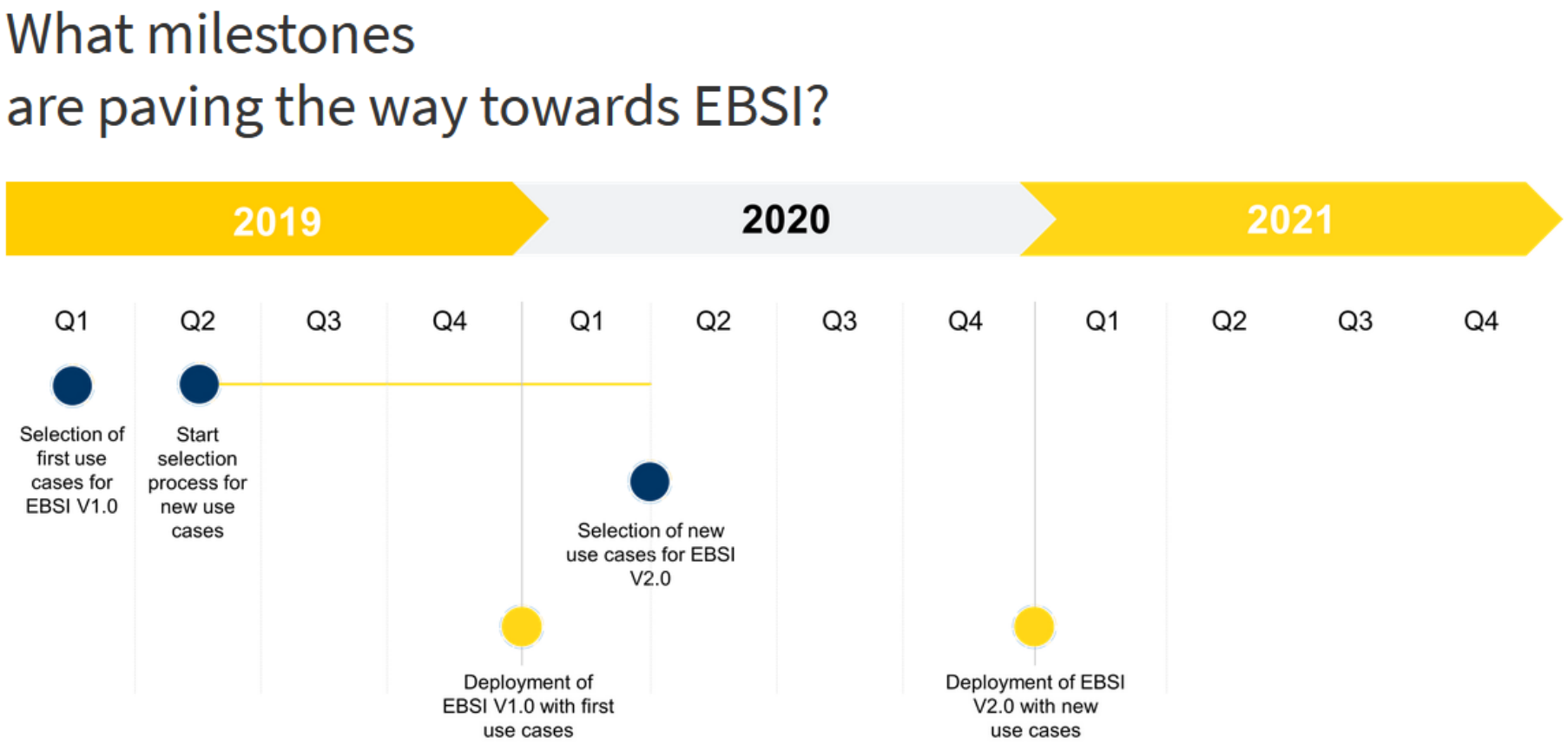
European Self-Sovereign Identity

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

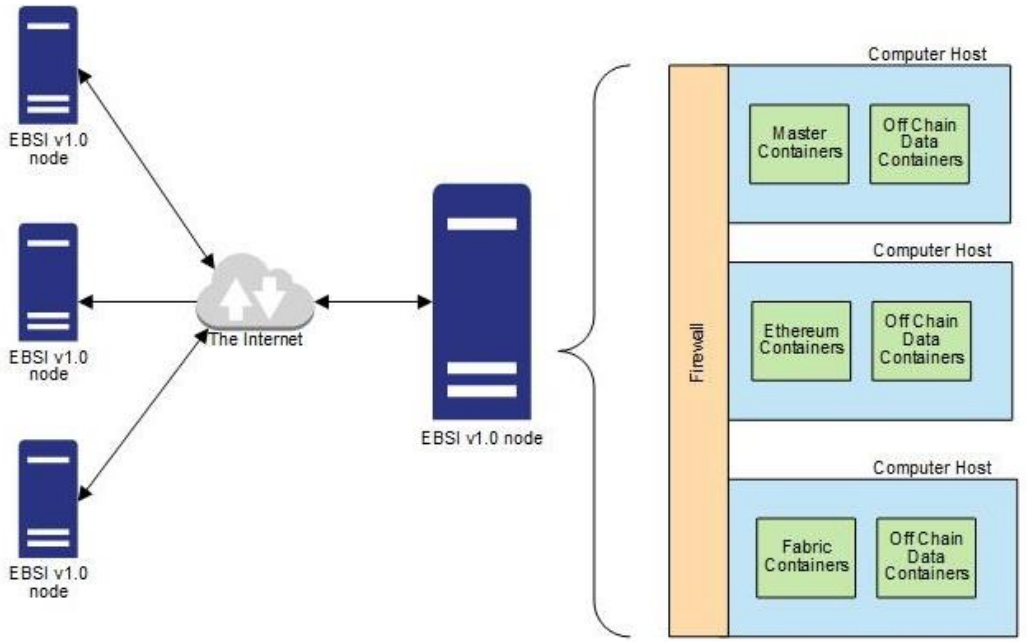
Leveraging blockchain technology to securely share data (e.g. IOSS VAT identification numbers and import one-stop-shop) amongst customs and tax authorities in the EU.

Zeithorizont ...



Node betreiben …

- 3 Hosts mit ca. 14 Services …



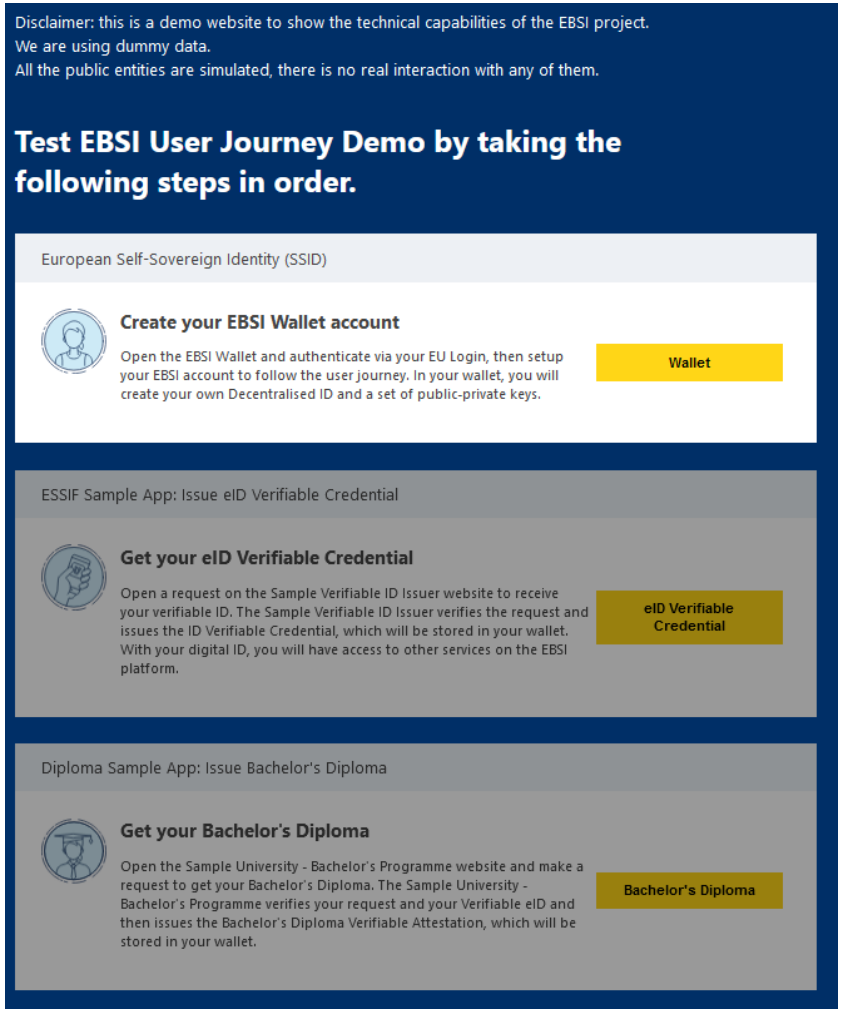
- https://ec.europ r+Hostir

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) leger (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

AUSTRIA PRO

An „functional test“ teilnehmen …

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



AUSTRIA PRO

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

AUSTRIA PRO

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