

# Arbeitskreis Blockchain

Allgemeines & Arbeitsgruppe Technik & Blockchain Lab

Dr. Christian Baumann

24.11.2022



# Agenda

- Begrüßung
- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Themen)
- News zum Thema NFTs
- eDAY22 und Blockchain Award 2022 - Nachlese NFTs
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - spontane Beiträge zu Projekten, Initiativen etc.

# Agenda

- Begrüßung
- **News zu „Austrian Public Service Blockchain“**
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Themen)
- News zum Thema NFTs
- eDAY22 und Blockchain Award 2022
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - spontane Beiträge zu Projekten, Initiativen etc.

# Austrian Public Service Blockchain

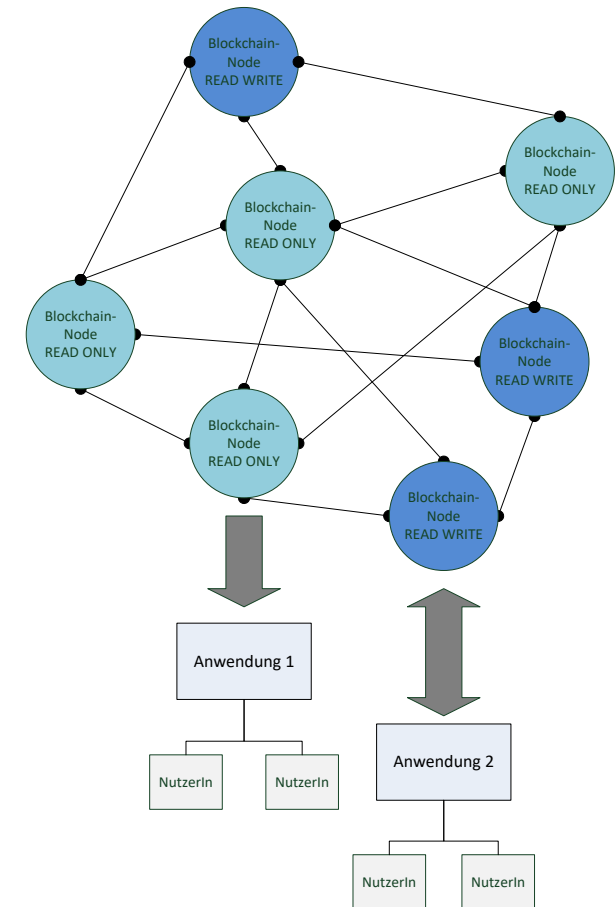
- Initiative von Institutionen der öffentlichen Verwaltung
- „Konsortium-Blockchain“ für unterschiedliche Usecases im „public service“ Bereich
  - Blockchain in Echtbetrieb seit 10/2019
- Konsortialpartner derzeit
  - WKO (Wirtschaftskammer): Daten-Zertifizierung
  - WU Wien: Daten-Zertifizierung
  - Stadt Wien: OGD Notarisierung
  - BRZ (Bundesrechenzentrum)
  - Nic.at (cert.at)
  - Gesundheitsministerium (BMSGPK)
    - **NEU: AGES (demnächst im Echtsystem)**  
**Gesundheitsbezogene Daten - OpenData**
  - OeKB (Österr. Kontrollbank) (zugesagt)
- Angefragt
  - FH St. Pölten, TU Wien ...

Austrian Public Service Blockchain (Nodes)	Test	Produktiv
BRZ (Bundesrechenzentrum)	ja (2)	ja (2)
Stadt Wien - MA01	ja (2)	ja (2)
WKO (Wirtschaftskammer Österreich)	ja	ja
nic.at/cert.at	ja	ja
WU (Wirtschaftsuniversität Wien)	ja	ja
BMSGPK (Gesundheitsministerium)		ja
AUSTRIAPRO	(ja)	
<b>Summe</b>	<b>8</b>	<b>8</b>

# Austrian Public Service Blockchain (APSB) Vereinbarung

- Inhalt (Finale Version 1.0 - 16.2.2022)

Management Summary .....	3
Einleitung.....	3
<b>1 Leitfaden .....</b>	<b>4</b>
1.1 Grundsätze der Infrastruktur .....	4
1.2 Technische Gründung.....	6
<b>2 Vereinbarung.....</b>	<b>7</b>
2.1 § 1 Gegenstand und Zweck des Austrian Public Service Blockchainsystems .....	7
2.2 § 2 APSB Architektur .....	7
2.3 § 3 Begriffsbestimmungen .....	8
2.4 § 4 Beitritt zur APSB .....	10
2.5 § 5 Rechte und Pflichten von Anwendungsverantwortlichen .....	10
2.6 § 6 Rechte und Pflichten des Knotenverantwortlichen.....	10
2.7 § 7 Technische und organisatorische Vorkehrungen.....	10
2.8 § 8 Haftungsregelung .....	11
2.9 § 9 Entzug der Teilnahme.....	11
2.10 § 10 Änderungen der Vereinbarung über die APSB .....	11
2.11 § 11 Schlussbestimmungen .....	11



# APSB Vereinbarung - Status



- Vereinbarung liegt in Version 1.0 vor
- Next Steps
  - Vorlage bei BLSG
  - -> Termin war im Sommer 2022
  - -> noch Unklarheiten seitens BLSG Mitglieder -> nächste Runde
  - Publish auf e-Government Reference Server als „Empfehlung“
- Anhänge
  - Vorlage zur Beitrittserklärung zur APSB
  - Technische Spezifikation (Implementierungs-Leitfaden)
    - Anforderungen Server, VPN, Multichain-Umgebung, Datenstruktur ...
  - Präsentationsunterlagen zur APSB für das Management

## Austrian Public Service Blockchain Leitfaden und Vereinbarung

**Doku-Klasse:**  
Konvention  
verbindlich

**Kurzbezeichnung:**  
APSB Vereinbarung

**Kurzbeschreibung:** Die Blockchain-Technologie kann die Unverfälschtheit von Daten aus technischer Sicht beweisen. Sie ist daher ein geeignetes Mittel, das Vertrauen in E-Government zu stärken.

Damit einzelne Projekte im öffentlichen Bereich die Technologie anwenden können, sowie Wissen zur Nutzung der Technologie aufbauen können, steht eine Blockchain-Infrastruktur für Österreich „Austrian Public Service Blockchain (APSB)“ für die Speicherung von nicht personenbezogenen Hashwerten zur Verfügung.

Im Leitfaden werden Standards und Empfehlungen zur Nutzung der APSB erklärt, die bei allen österreichischen Verwaltungen für den Betrieb von Blockchain-Knoten und darauf basierenden Anwendungen zur Anwendung kommen können.

In der Vereinbarung werden Gegenstand und Zweck der APSB, Architektur, Rechte und Pflichten, sowie Haftung der APSB-Teilnehmer:innen erläutert.

**Verfasst von:** Alexander Banfield-Mumb, BMDW  
Alfred Taudes, Wirtschaftsuniversität Wien /Austrian Blockchain Center  
Andreas Abraham, A-SIT  
Brigitte Lutz, Stadt Wien  
Christian Baumann, AustriaPro  
Christina Schadauer, OeKB  
Gerhard Laga, WKO  
Heinz Wachmann, OeKB  
Matthias Lichtenthaler, BRZ  
Petra Stummer, Land NÖ  
Selin Madran, Stadt Wien

**Projektteam/Arbeitsgruppe:** Austrian Public Service Blockchain

**Version / Datum:** V1.0 / 16.02.2022

**Doku-Stadium:** Ergebnis der AG

## APSB Grundsätze

- Die verwendeten Konsensalgorithmen stellen sicher, dass **kein energieverwendendes Mining** betrieben wird und die Infrastruktur auch umwelt- und ressourcenschonend gestaltet ist.
- **Made in Austria**, aber unter Beobachtung der EU Aktivitäten
- Anwendung von **Open Source Software** (Multichain)
- **Datenschutz**: Personenbezogene Daten werden offchain gespeichert und sind nicht Gegenstand dieser Infrastrukturen.

# Einsatz im Gesundheitsministerium (BMSGPK)

- Das BMSGPK betreibt seit 6/2022 einen Blockchain-Node im Rahmen der „Austrian Public Service Blockchain“.
- Seit 8/2022 läuft die erste Anwendung „Daten-Zertifizierung für OpenData“.
  - Dabei werden Daten des Covid19- und des Impf-Dashboard vollautomatisch zertifiziert (notarisiert).
  - „Transparenz für Daten im e-Health Bereich“
- Weitere Anwendungen sind in Planung.
- Das BMSGPK ~~wird~~ ebenfalls ein öffentlich zugängliches Verifikationsservice ~~betreiben~~.
  - **NEWS:** <https://verify.ehealth.gv.at/>
- Parallel dazu: EU weites Projekt x-eHealth („Blockchains in e-Health“)
- -> Hackathon ...



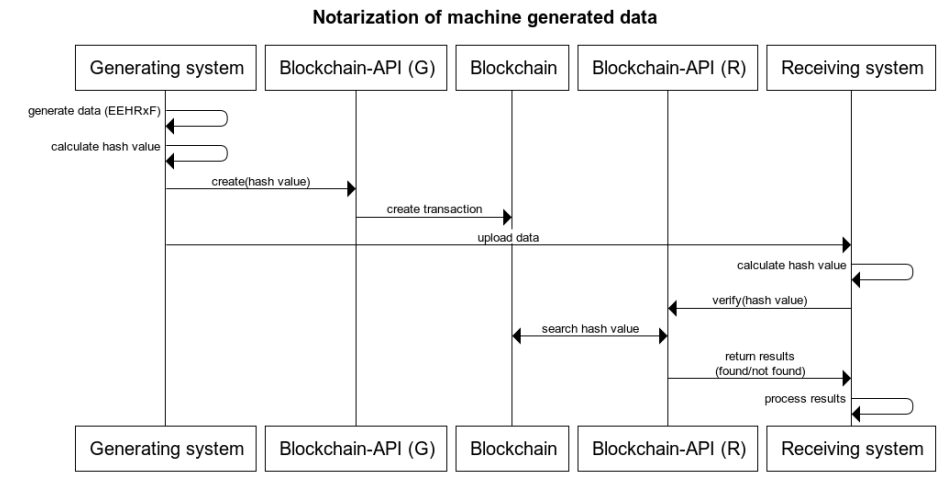
# Hackathon „Rare diseases and cancers“

- Veranstalter: X-eHealth Network
  - <https://www.x-ehealth.eu/>
- Teilnehmer aus EU Raum
  - U.a. Ministry of Health, Austria
- Titel: Blockchain based Notarization
- Topic: Notarization of machine generated data
  - (in the context of e-Health)
  - Define processes
  - Design components for a prototype/PoC
  - Implementation



# Notarization of machine generated data 1/2

- **Generating system**
  - Generates data (e.g. in EEHRxF) \*
  - Notarizes data
    - calculates hash value and stores it on blockchain
  - Sends data to receiving system
- **Receiving system**
  - Verifies integrity of data
    - calculates hash value, looks it up on blockchain
    - checks timestamp and public key of sender
  - Processes data

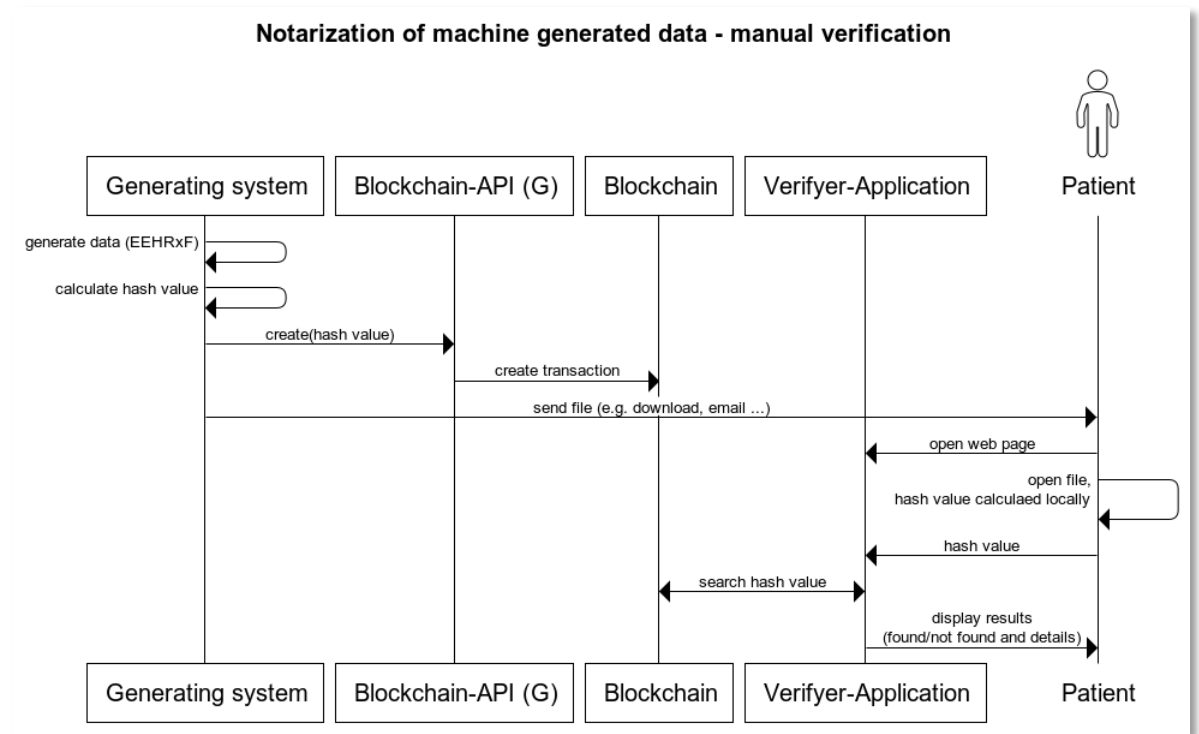


(\*) European Electronic Health Records eXchange Format

ALL formats can be used: HL7, IHE, ICD-\*, Snomed, Loinc ..., PDF, Logfiles, DB dumps ...

# Notarization of machine generated data 2/2

- “Receiving system” = patient
  - Documents e.g.
    - Lab reports
    - Sickness certificates
    - Discharge reports
    - ...
  - Verifies integrity of data
    - Using a Web-GUI



# Components (provided/implemented)

- Access to a blockchain system (already existing) - (DatNoS-Testchain - AP-Lab)
  - Special „stream“ for the data to be processed in the context of this hackathon
- REST-API for notarization and verification
  - example scripts and API keys for interested parties
- Prototype scripts for
  - generating/sending system
  - receiving/processing system
- Web-GUIs for
  - viewing the blockchain stream
  - manual verification of files
- Prototype: <https://test.baumann.at/xeh/>

## HIM-AT prototype for "x-eHealth-Hackathon 2022"

### Links

[Stream viewer](#)

[Verifier \(Web-GUI\)](#)

[Example files for verification](#)

[FHIR Uploader \(for manual uploading\)](#)

[API \(you need an API-Key\)](#)

### Used Blockchain addresses (public keys)

1UsW6Fq469dRGbbVr28ou31c7mjNFzQHcSPJG assigned to Austrian prototype system "HIM-AT"

187w4eauq9yV22hvPqiK5Fr3KTH8REUw1v7yBR assigned to Cyprus eHealth4u Intergration

# Spontane Kooperation ...

- Integration of
  - Cyprus eHealth4U PDF „Discharge Summary“ with
  - Notarization in HIM-AT prototype system

Alexandra Georgiou <small>Female / 34 Year Old / 99123456 / Nicosia</small>		Patient Summary
Medical Personal History		
Allergies & Intolerances		
Intolerance - Drug		
Type	Propensity to adverse reactions to drug	
Description	Intolerance to ALDOSTERONE ANTAGONISTS AND OTHER POTASSIUM-SPARING AGENTS eosinophilia and systemic symptoms	
Criticality	Medium Risk	
Code	ALDOSTERONE ANTAGONISTS AND OTHER POTASSIUM-SPARING AGENTS	
Clinical Status	Active	
Recorded Date	11/20/2010	
Onset	10/20/2010	

<https://www.x-ehealth.eu/hackathon-for-rare-diseases-and-cancers/>

DocNoS - Data View - Stream "x-eHealth-Hackathon"	
Select Key	
<a href="#">[all]</a> - <a href="#">xeht/1</a> - <a href="#">xeht/2</a> - <a href="#">xeht/3</a>	
Key: <a href="#">xeht/2</a>	
2 of 2 items	
<a href="#">first</a> - <a href="#">prev</a> - <a href="#">next</a> - <a href="#">last</a>	
<b>Publishers</b>	187w4eau9yV22hvPqIK5Fr3KTH8REUw1v7yBR
<b>Key 0</b>	<a href="#">id2f2e9314-5a1f-4e51-8821-352cb87b8824</a>
<b>Key 1</b>	<a href="#">sha256:5cbca4587a444543a9b02f0b7c951b632ae786d4c4316a14c0979236df071206</a>
<b>Key 2</b>	<a href="#">xeht/2</a>
<b>JSON data</b>	<pre>{   "timeStamp": "2022-10-03T18:45:38+02:00",   "client": "xeht/2",   "version": "DocNoS-v1.1",   "data": {     "id": "2f2e9314-5a1f-4e51-8821-352cb87b8824",     "hashes": {       "sha256": "5cbca4587a444543a9b02f0b7c951b632ae786d4c4316a14c0979236df071206"     }   },   "remarks": "Cyprus eHealth4u Intergration - Discharge Summary - X-eHealth Hackathon" }</pre>
<b>Transaction</b>	2a7efe71c8e22a448337c4cae7c924c7b884bcc5d552a2da9aafc615fcbac47f
<b>Blocktime</b>	2022-10-03T18:44:24+02:00
<b>Blockhash</b>	00e0eb163117dc166d56ed03990584b044b7503c9a28b8b9f62a00d8cdfaf6e8

# Agenda

- Begrüßung
- News zu „Austrian Public Service Blockchain“
- **News zu „Datenzertifizierung für die Privatwirtschaft“**
- News aus dem TestLab (Anwendungsfälle, technische Themen)
- News zum Thema NFTs
- eDAY22 und Blockchain Award 2022
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - spontane Beiträge zu Projekten, Initiativen etc.

# „Daten-Zertifizierung“ für die Privatwirtschaft

- Initiative "Private Sector Blockchain"
- Unterstützung seitens AUSTRIAPRO (WKO)
- Ziele
  - „Konsortialblockchain zur Zertifizierung von Daten“
  - Aufbau einer dauerhaften und sicheren Blockchain-Infrastruktur für Österreichs Wirtschaft
  - Einrichtung und Moderation eines offenen Stakeholder-Forums zum Aufbau und Steuerung der Infrastruktur

# BCI

Blockchain Initiative Austria

- Blockchain Initiative Austria
  - Offiziell gegründet 1/2021
- Aktuell (11/2022)
  - **21 Mitglieder & 1 Netzwerkpartner**
- <https://www.bc-init.at/>
  - Mitgliederliste
  - Vereinsstatuten
  - Beitrittsantrag
  - Systembeschreibung & Rahmenbedingungen
  - Aktualisiert: DocNoS REST-API
  - ...



## Aktuelle Mitgliederliste

ABC Research GmbH - Austrian Blockchain Center	
Algordanza Erinnerungsdiamanten Handels GmbH	
AUSTRIAPRO - Verein zur Förderung standardkonformer E-Business Lösungen	
baumann.at - Blockchain Consulting & Development	
Bridge of Trust - digital	
DEUDAT GmbH - Datenschutz und Informationssicherheit - Anwendung: Notarisierung	
Infinite Trust Digital GmbH	
IoT Austria - The Austrian Internet of Things Network	
IVM Technical Consultants GmbH	
Kosch & Partner Rechtsanwälte GmbH Anwendung: Digitale Zertifizierung	
RBKS - Dipl.-Ing. Roman Bruckberger-Koch	
SEC Consult Unternehmensberatung GmbH - Anwendung: ForensicForever	
Securikett Ulrich & Horn GmbH	
SIMTOOLS GmbH	
SYNERCON GmbH	
VIM Internetdienstleistungen GmbH	
Woschitz group GmbH - News-Beitrag vom 5.5.2021	

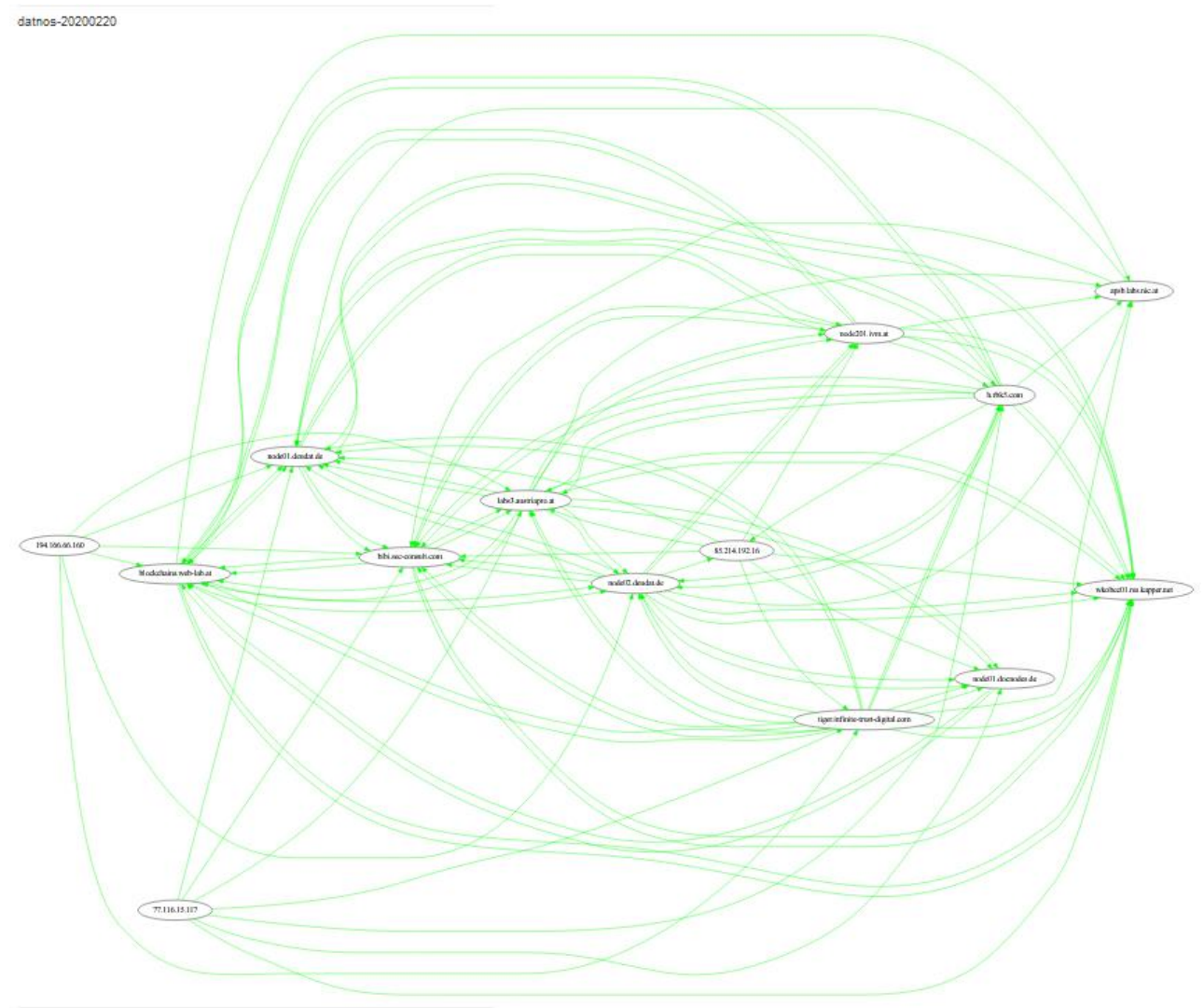
## Ehrenmitglieder

Prof. Alfred Taudes - Institute for production engineering & Research Institute for Cryptoeconomics - WU Wien	
---	--



# Blockchain-Infrastruktur

- Blockchain in Echtbetrieb seit 20.2.2020
  - **Aktuell 14 Knoten**
- Erster Use-Case: „Daten-Zertifizierung“
- Mehrere Anwendungen in Echtbetrieb
- Bisher ca. (11/2022)
  - **217.000 Blöcke**
  - **287.000 Transaktionen**
- <https://www.bc-init.at/blockchain>



# NEWS

- Neuer Usecase von (docnodes.de)
  - Koppelung zu einem Datenraum-Portal
    - Mandantenfähig
    - Entweder für Zeitraum zu „mieten“ oder On-Premise
  - Notarisierung von
    - Dokumente (Versionen)
    - Metadaten (Zugriffe)
    - ...
  - Status
    - Testbetrieb erfolgreich
    - Implementierung in Echtssystem ongoing

# Agenda

- Begrüßung
- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- **News aus dem TestLab (Anwendungsfälle, technische Themen)**
- News zum Thema NFTs
- eDAY22 und Blockchain Award 2022
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - spontane Beiträge zu Projekten, Initiativen etc.

# NEWS

- „Futurelab“ eines Anbieters von Postdienstleistungen
  - Kontakt zur AustriaPro aufgenommen
  - Interesse an Teilnahme an der DatNoS Blockchain
  - 2 Meetings
    - Vorgespräche und Usecases definiert
  - Aktuell: Onboarding ins Testsystem

# „Dual Verify“

- Bisher: getrennte Verifikation für
  - APSB: WKO, Wien, WU, BMGSPK ...
  - PSBC: proof.li, DEUDAT, ITD, K&P ...
- Ziele
  - Verbesserung Usability
  - engere Koppelung der Systeme
- Status
  - System im Echtbetrieb
  - <https://datenzertifizierung.at/>
- **NEWS: interne Optimierungen, Optik**

The screenshot shows two overlapping windows from the 'Blockchain Datenzertifizierung' application. The background window is the main interface with a '+ Erstellen' button and a magnifying glass icon labeled 'Überprüf'. It contains a document name 'Dokumentation\_Nachträgliches\_Ubermi...', a hash field with the value '36d965ff34729bc51a968fc018e41bce', and a 'Transaktions-ID (optional) ...' field. A red button at the bottom says 'Jetzt Dokument überprüfen'. The foreground window shows a successful verification result with a green checkmark, the document name, the creation time 'Zuerst erstellt am 08.09.2021 12:16', the 'Digitaler Fingerabdruck (Hash)' '36d965ff34729bc51a968fc018e41bce', and the 'Transaktions-ID' '618d504cc592954eaefe3490c9c2304'. It has 'Zurück' and 'Details ansehen' buttons.

The screenshot shows the 'proof.li' interface for 'Notarisierung verifizieren'. It includes a header with the 'proof.li' logo and 'Erstellen Verifizieren' buttons. The main text explains that users can verify if a document was notarized by checking its digital fingerprint (hash) against the blockchain. It provides instructions to either select a file (noting it won't be uploaded) or enter a hash or transaction ID. A file selection dropdown shows '20220508\_MT\_20222308-11242348.txt'. Below, there are input fields for the hash (containing '764c6699330864f4e653ae267152db05c175e38926dc6ba7525c83f214378407') and the transaction ID. A blue 'Verifizieren' button is at the bottom.

# Verifikation mittels „Dual Verify“



Blockchain-Service Datenzertifizierung

## Überprüfen einer Datenzertifizierung

Sie können hier überprüfen ob/wann ein Dokument zertifiziert (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 manuell (mit Copy/Paste) ein.

Es wird automatisch in den beiden Blockchain-Systemen **Austrian Public Service Blockchain** (aka Blockstempel) und **Private Sector Blockchain** (aka DatNoS) gesucht. Details dazu [siehe hier](#).

Zu verifizierende Datei auswählen, um den Hashwert im Browser zu berechnen. Die Datei wird dabei NICHT auf den Server hochgeladen.

Durchsuchen... Keine Datei ausgewählt.

Digitaler Fingerabdruck (Hashwert sha256)

a05ad3a24a9e65210eb5914a34f82f611d3cf9bbcce307fdb1ccc192bb2fd8b

Alternativ Transaktions-ID eingeben:

Optional: Alle Details anzeigen

Dokument verifizieren

© - 2022 - [Datenschutzerklärung](#) - [Offenlegung](#)

<https://datenzertifizierung.at/>



## Ergebnis der Überprüfung

Es wurde in den beiden Blockchain-Systemen **Austrian Public Service Blockchain** (aka Blockstempel) und **Private Sector Blockchain** (aka DatNoS) gesucht. Falls das gleiche Dokument mehrfach zertifiziert wurde, ist der zeitlich älteste Eintrag der relevanteste.

## Zusammenfassung



Hashwert "05952777457d5ef3716c9c9dac750038e9406a3160695d65ec1dfe7c421a0c8a" gefunden.

## Austrian Public Service Blockchain

Es wurde ein Eintrag gefunden, d.h. das Dokument mit dem gesuchten Hashwert wurde zum angegebenen Zeitpunkt in diesem System digital zertifiziert.

Eintrag 1/1

Zeitstempel	2022-07-12T09:39:17+02:00
Transaktions-ID	8a64ff6b8a6b07a171fe7452ed712774f2513f0492273695fd2137edace329e7
Hashwert (sha256)	05952777457d5ef3716c9c9dac750038e9406a3160695d65ec1dfe7c421a0c8a
Blockzeit	2022-07-12T09:39:25+02:00
Blockhash	00145e8e3c06a069c8e0c23ba21eb80ff86a3e266c847bb69009c337aac92dc8
Bestätigungen	12417

## Private Sector Blockchain

Es wurde ein Eintrag gefunden, d.h. das Dokument mit dem gesuchten Hashwert wurde zum angegebenen Zeitpunkt in diesem System digital zertifiziert.

Eintrag 1/1

Zeitstempel	2022-07-12T09:41:30+02:00
Transaktions-ID	a3abaae990042aa58e2cc209e8c8d2fc19f9d11b222069300c2f09818ec5f009
Hashwert (sha256)	05952777457d5ef3716c9c9dac750038e9406a3160695d65ec1dfe7c421a0c8a
Blockzeit	2022-07-12T09:41:33+02:00
Blockhash	006f93cfd535bd35d1f0fd3b808d7a85fc0c69df18d7a83146bb626f261ee9
Bestätigungen	21616

Zurück

# Datenzertifizierung - Infoseite



Blockchain-Service Datenzertifizierung

## Details

Mit dem Blockchain-Datenzertifizierungsservice der WKÖ lassen sich Daten einfach, sicher und kostenlos digital zertifizieren. Somit sind Unternehmensdaten geschützt und ihre Echtheit belegt. Unabhängig vom Dateiformat erhalten Daten hierbei einen Zeitnachweis, wann sie entstanden sind, vorgelegen oder verändert wurden.

Es werden zwei - auf gleichen technologischen Grundlagen arbeitende - Servicetools angeboten: die „Austrian Public Service Blockchain“ und die „Private Sector Blockchain“. Der Unterschied liegt in den Betreibern der Blockchain Knoten - wie die Namen andeuten, sind dies einmal öffentliche Einrichtungen und einmal private Unternehmen und Institutionen. Für die Servicenutzer:innen macht dies keinen Unterschied.

## Austrian Public Service Blockchain

Bei der APSB handelt es sich um ein Konsortium aus Institutionen der öffentlichen Verwaltung, die die Blockchain-Knoten betreiben. Dabei sind u.a.

- Wirtschaftskammer Österreich - [Datenzertifizierung](#) auf [mein.wko.at](#)
- Wirtschaftsuniversität Wien - [Datenzertifizierung](#) für WU-Angehörige
- nic.at/cert.at - [Blogbeitrag](#)
- Stadt Wien
- BM Soziales, Gesundheit, Pflege, Konsumentenschutz
- Bundesrechenzentrum - [BRZ TechBlog #3](#)

## Private Sector Blockchain

Die PSBC ist das privatwirtschaftliche Pendant zur APSB und basiert auf derselben Technologie. Die Knoten werden von Mitgliedern des Vereins "[Blockchain Initiative Austria](#)" betrieben. Applikationen betreiben u.a.

- proof.li - [Referenzimplementierung](#) der Blockchain Initiative Austria
- DEUDAT GmbH - [Notarisierung](#)
- docnodes GmbH - [Dokumenten-Notarisierung](#)
- Kosch & Partner Rechtsanwälte GmbH - [Digitale Zertifizierung](#)

# Prüfzertifikate als NFT

- NFT als „digitaler Zwilling“
- Ablauf
  - Dokument als PDF generieren
  - Optional digital signieren
  - Metadaten erstellen
  - Metadaten und Dokument im IPFS ablegen
  - Smart Contract aufrufen -> NFT wird „geminted“
- Ergebnis
  - Dokument + Metadaten sind unveränderbar im IPFS abgelegt.
  - NFT als digitaler Zwilling des Dokumentes befindet sich im Wallet des Erstellers und kann an ein anderes Wallet (z.B. des Kunden) transferiert werden.

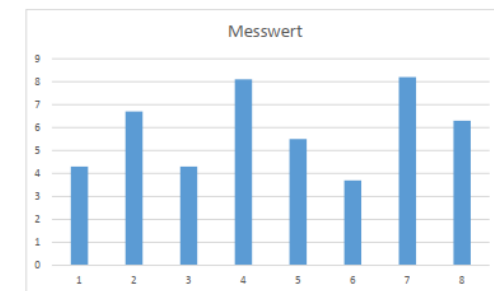
25.6.2022

## Zertifikat

Prüfung laut ISO 12345:67

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Prüfung	Messwert
1	4,3
2	6,7
3	4,3
4	8,1
5	5,5
6	3,7
7	8,2
8	6,3



Signature	Dr. Christian Krammer
<b>Signature-UTC</b>	2022-06-25T10:00:00Z
<b>Verification</b>	Information about the verification of the certificate signature can be found at: <a href="https://www.example.com/verify">https://www.example.com/verify</a>
<b>Note</b>	This document is signed with a qualified electronic signature. According to Art. 26 para. 2 of the Regulation (EU) No 910/2014 of 23. July 2014, 'Qualified-signatory', it shall have the equivalent legal effect of a handwritten signature.



# Details zum NFT

- Smart Contract läuft auf Polygon (Testnetz Mumbai)
  - Standard ERC721, Erweiterungen
- Alle Details über Blockchain-Explorer einsehbar
  - Transaktion:  
<https://mumbai.polygonscan.com/tx/0x6e73714dd560f42c7e4dc214173a064be8b15b18a9554527d8ea1071ccbe8774>
  - Smart contract address:  
<https://mumbai.polygonscan.com/address/0xb145568dedcefa5f76d46f8330366e5ed3f7c9b5>
  - NFT address  
<https://mumbai.polygonscan.com/token/0xb145568dedcefa5f76d46f8330366e5ed3f7c9b5?a=4>

# Ablage der Daten

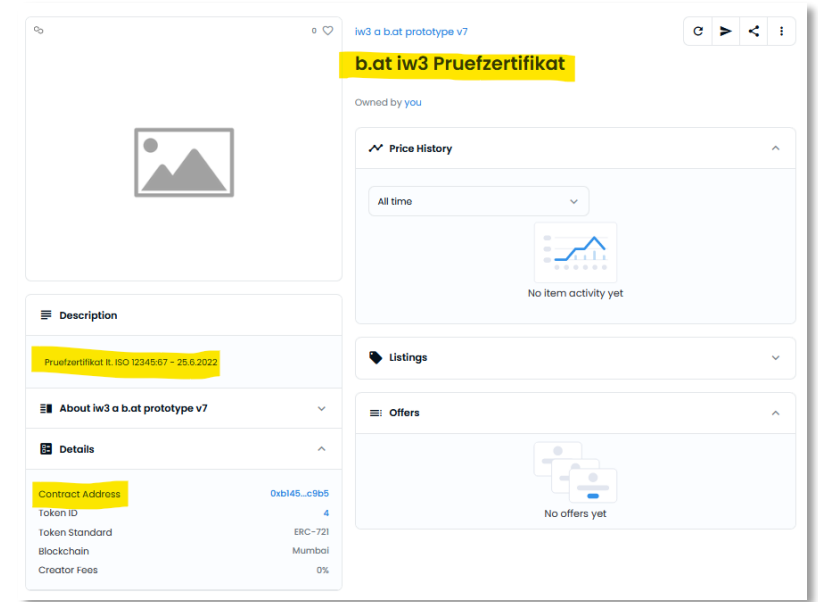
- IPFS: damit eindeutig, unveränderbar, unlöschbar
- Metadaten (im NFT verlinkt)
  - `ipfs://bafybeibhipsryqokeg4nqnwycsxu6ydme7yrjqws37qmmatvdzxpjgm4fi/metadata.json`
  - <https://ipfs.io/ipfs/bafybeibhipsryqokeg4nqnwycsxu6ydme7yrjqws37qmmatvdzxpjgm4fi>

```
name: "b.at iw3 Pruefzertifikat"
description: "Pruefzertifikat lt. ISO 12345:67 - 25.6.2022"
image: "ipfs://bafybeid7goxwwpmqaldlxqbkpwnf3tjuxdkoijuapt7cmigzcwvgsr74/Pruefzertifikat_13124_20220625_signed.pdf"
```

- Zertifikat
  - `ipfs://bafybeid7goxwwpmqaldlxqbkpwnf3tjuxdkoijuapt7cmigzcwvgsr74/Pruefzertifikat_13124_20220625_signed.pdf`
  - <https://ipfs.io/ipfs/bafybeid7goxwwpmqaldlxqbkpwnf3tjuxdkoijuapt7cmigzcwvgsr74>

# „Darstellung“

- Beispiel OpenSea
  - Schönheitsfehler: PDF kann dort nicht direkt angezeigt werden
  - Das NFT könnte aber zusätzlich ein Image enthalten
  - Link zu Explorer -> tokenURI -> metadaten
  - <https://testnets.opensea.io/assets/mumbai/0xb145568dedcefa5f76d46f8330366e5ed3f7c9b5/4>



```
12. tokenURI
tokenId (uint256)
4
Query
string
[ tokenURI method Response ]
>> string : ipfs://bafybeibhipsryqokeg4nqnwycsxu6ydm7yrjqws37qmmatvdzxpjgm4fi/metadata.json
```

# Zusammenfassung - Dokumente als NFTs

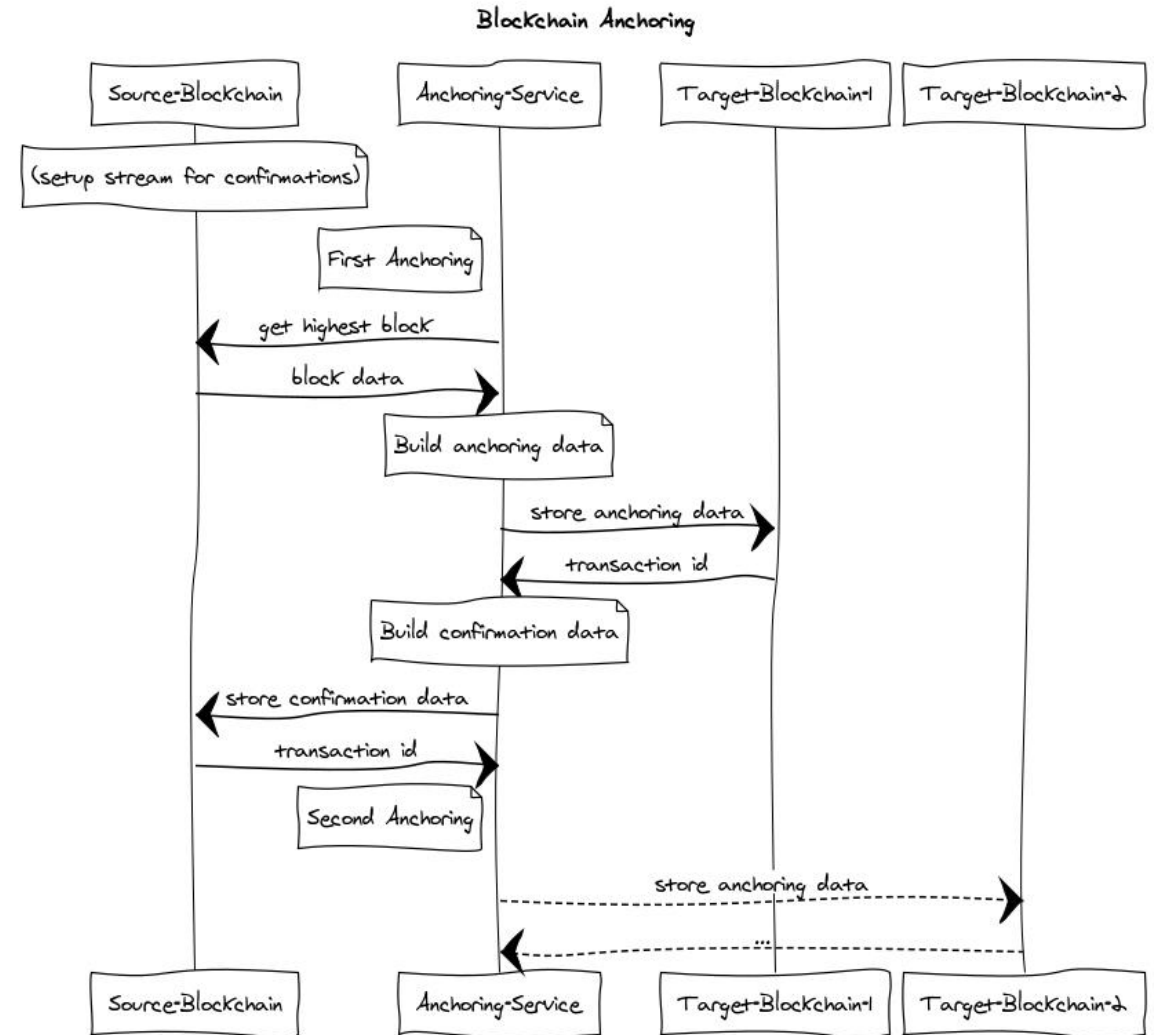
- Dokumente (z.B. PDF) können als NFTs „geminted“ werden.
  - NFT kann an Dritte übertragen werden.
- Dokument und Metadaten „unlöschar“ im IPFS abgelegt.
  - Metadaten können beliebige Informationen in strukturierter Form enthalten
- Alle Informationen können über gängige Tools (Blockchain-Explorer) oder (zu erstellende) dApps abgerufen werden.
- NFT als digitaler Zwilling ist Beweis für
  - Zeitpunkt der Erstellung
  - Ersteller: über Wallet-Adresse und optional Digitale Signatur

# Erhöhung des Vertrauens durch „Anchoring“

- Notarisieren des aktuellen Zustandes einer Blockchain in einer anderen Blockchain („snapshot“)
  - Typischerweise um eine „kleine“ Blockchain ...
  - ... in eine „große“ zu verankern
  - Z.B. private oder Konsortiumchain mit wenigen Nodes in eine public Blockchain
- Zweck: Nachweis dass die Source-Chain
  - nicht manipuliert wurde
  - bzw. potentielle Manipulationen erkannt würden
- Daten des jeweils aktuellen Blocks
  - Blocknummer
  - Block-Hash
  - Zeitstempel

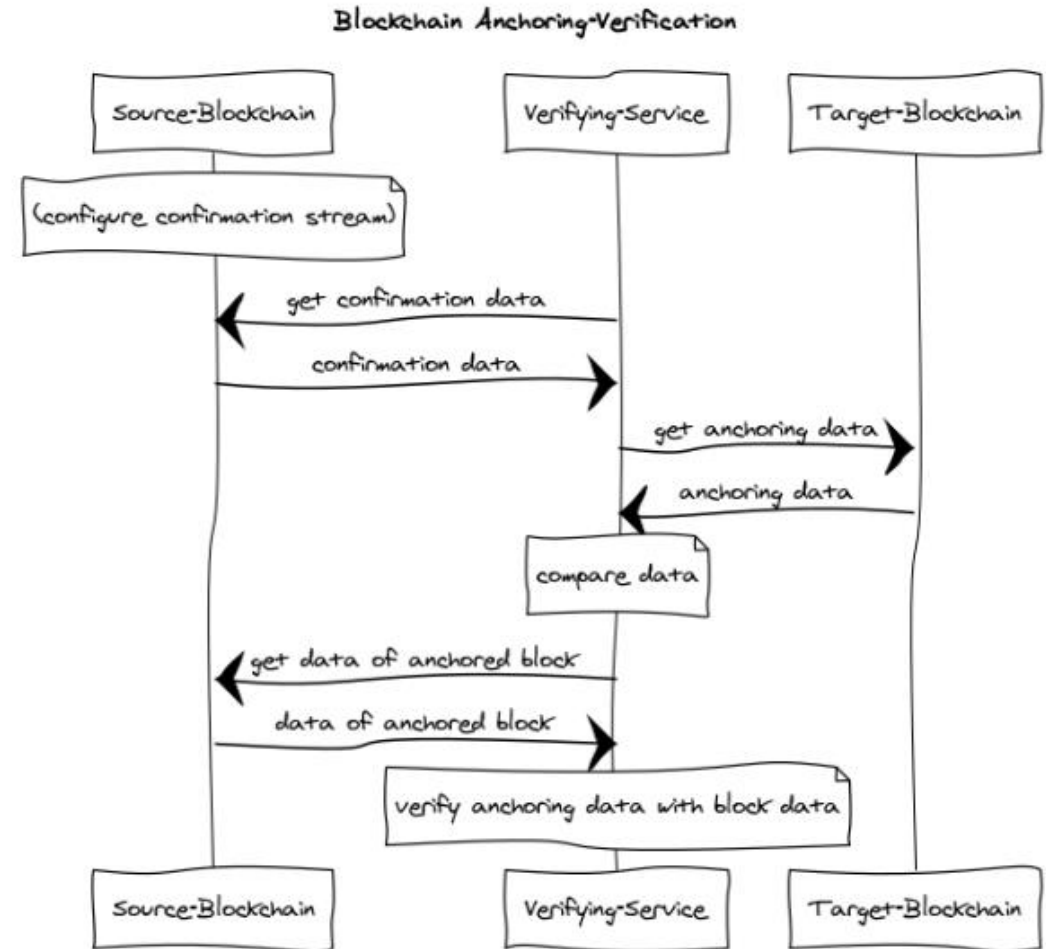
# Anchoring - Ablauf

- Aktuelle Blockdaten von Source-Chain abfragen
- Daten aufbereiten (Json ...)
- Transaktion in Target-Chain/s durchführen
- Ergebnis (Bestätigung) in Source-Chain protokollieren



# Anchoring - Ablauf Verifikation

- Bestätigung aus Source-Chain lesen
- Anchoring data in Target-Chain suchen
- Daten vergleichen
- Blockdaten in Source-Chain verifizieren



# Anchoring - Status 11/2022

- Prototypische Implementierung vorhanden
- Erkenntnisse aus Testbetrieb
  - Noch diverse Erweiterungen/Features nötig
  - Implementierung ongoing
  - Basis: Dual-Verify (bereits beide Schnittstellen parallel)
- Diskussionen zu Target-Chains
  - Klar
    - APSB -> PSBC
    - PSBC -> APSB
  - Offen
    - Layer 2 Chain (Polygon): geringe Kosten, schnelle Transaktionen
    - Ethereum 2.0?
      - „Merge“ ist erfolgt
      - **Kaum/keine Verbesserungen bei Kosten und Geschwindigkeit?**
      - -> Analyse läuft weiter ...



# Praxisbericht Datenzertifizierung 1/2

- „Cloud-Lösung“ ändert Files beim Abrufen ...
- Ablauf
  - Dokument (Zertifikat über Absolvierung eines „teaching programs“) wird generiert (PDF) und notariert (APSB).
  - Dokument wird an Studenten übermittelt
  - Dokument wird in einer „Cloud-Lösung“ gespeichert
  - Nach ein paar Monaten wird es aus der Cloud abgerufen und (nochmals) übermittelt.
  - -> Verifikation auf der APSB schlägt fehl
  - (Originaldokument war gsd. noch in ursprünglicher Anwendung gespeichert)

# Praxisbericht Datenzertifizierung 2/2

- Analyse
  - PDF Viewer zeigt Dokumenteneigenschaften
  - Binärer Vergleich zeigt Unterschiede
    - Zeitstempel
    - Tool-Version
    - Interne ID (UUID)
  - -> Daher ist Hashwert anders

- Erkenntnis:  
„Cloud-Tool“ ändert PDF  
beim Abrufen
- Admins untersuchen Verhalten
- Originalfile konnte korrekt  
verifiziert werden

Erstellt am: 31.03.2022 10:15:41

Geändert am: 20.10.2022 13:26:54

Anwendung: Canon iR-ADV C5550 III PDF

Erweitert

PDF erstellt mit: Adobe PSL 1.3e for Canon

PDF-Version: 1.4 (Acrobat 5.x)

```
99B8: 3D 22 41 64 6F 62 65 20 |="Adobe
99C0: 58 4D 50 20 43 6F 72 65 |XMP Core
99C8: 20 37 2E 31 2D 63 30 30 | 7.1-c00
99D0: 30 20 37 39 2E 34 32 35 |0 79.425
99D8: 64 63 38 37 2C 20 32 30 |dc87, 20
99E0: 32 31 2F 31 30 2F 32 37 |21/10/27
99E8: 2D 31 36 3A 32 30 3A 33 |-16:20:3
99F0: 32 20 20 20 20 20 20 20 |2
99F8: 20 22 3E 0A 20 20 20 3C | ">. <

99B8: 3D 22 41 64 6F 62 65 20 |="Adobe
99C0: 58 4D 50 20 43 6F 72 65 |XMP Core
99C8: 20 38 2E 30 2D 63 30 30 | 8.0-c00
99D0: 31 20 37 39 2E 33 32 38 |1 79.328
99D8: 66 37 36 65 2C 20 32 30 |f76e, 20
99E0: 32 32 2F 30 38 2F 30 31 |22/08/01
99E8: 2D 31 39 3A 31 30 3A 32 |-19:10:2
99F0: 39 20 20 20 20 20 20 20 |9
99F8: 20 22 3E 0A 20 20 20 3C | ">. <

99B8: 30 32 32 2D 30 33 2D 33 |022-03-3
99BF0: 31 54 31 31 3A 33 30 3A |1T11:30:
99BF8: 35 36 2B 30 32 3A 30 30 |56+02:00
99C00: 3C 2F 78 6D 70 3A 4D 6F |</xmp:Mo
99C08: 64 69 66 79 44 61 74 65 |difyDate
99C10: 3E 0A 20 20 20 20 20 20 |>.
99C18: 20 20 20 3C 78 6D 70 3A | <xmp:
99C20: 4D 65 74 61 64 61 74 61 |Metadata
99C28: 44 61 74 65 3E 32 30 32 |Date>202
99C30: 32 2D 30 33 2D 33 31 54 |2-03-31T
99C38: 31 31 3A 33 30 3A 35 36 |11:30:56

99B8: 30 32 32 2D 31 30 2D 32 |022-10-2
99BF0: 30 54 31 34 3A 32 36 3A |0T14:26:
99BF8: 35 34 2B 30 32 3A 30 30 |54+02:00
99C00: 3C 2F 78 6D 70 3A 4D 6F |</xmp:Mo
99C08: 64 69 66 79 44 61 74 65 |difyDate
99C10: 3E 0A 20 20 20 20 20 20 |>.
99C18: 20 20 20 3C 78 6D 70 3A | <xmp:
99C20: 4D 65 74 61 64 61 74 61 |Metadata
99C28: 44 61 74 65 3E 32 30 32 |Date>202
99C30: 32 2D 31 30 2D 32 30 54 |2-10-20T
99C38: 31 34 3A 32 36 3A 35 34 |14:26:54

99B8: 30 32 32 2D 30 33 2D 33 |022-03-3
99BF0: 31 54 31 31 3A 33 30 3A |1T11:30:
99BF8: 35 36 2B 30 32 3A 30 30 |56+02:00
99C00: 3C 2F 78 6D 70 3A 4D 6F |</xmp:Mo
99C08: 64 69 66 79 44 61 74 65 |difyDate
99C10: 3E 0A 20 20 20 20 20 20 |>.
99C18: 20 20 20 3C 78 6D 70 3A | <xmp:
99C20: 4D 65 74 61 64 61 74 61 |Metadata
99C28: 44 61 74 65 3E 32 30 32 |Date>202
99C30: 32 2D 30 33 2D 33 31 54 |2-03-31T
99C38: 31 31 3A 33 30 3A 35 36 |11:30:56

99B8: 30 32 32 2D 31 30 2D 32 |022-10-2
99BF0: 30 54 31 34 3A 32 36 3A |0T14:26:
99BF8: 35 34 2B 30 32 3A 30 30 |54+02:00
99C00: 3C 2F 78 6D 70 3A 4D 6F |</xmp:Mo
99C08: 64 69 66 79 44 61 74 65 |difyDate
99C10: 3E 0A 20 20 20 20 20 20 |>.
99C18: 20 20 20 3C 78 6D 70 3A | <xmp:
99C20: 4D 65 74 61 64 61 74 61 |Metadata
99C28: 44 61 74 65 3E 32 30 32 |Date>202
99C30: 32 2D 31 30 2D 32 30 54 |2-10-20T
99C38: 31 34 3A 32 36 3A 35 34 |14:26:54

9D30: 3A 49 6E 73 74 61 6E 63 |:Instanc
9D38: 65 49 44 3E 75 75 69 64 |eID>uuid
9D40: 3A 35 33 66 33 33 66 36 |:53f33f6
9D48: 30 2D 39 62 64 65 2D 34 |0-9bde-4
9D50: 39 39 32 2D 38 39 63 37 |992-89c7
9D58: 2D 38 30 35 65 32 39 37 |-805e297
9D60: 36 31 64 61 66 3C 2F 78 |6ldaf</x
9D68: 6D 70 4D 4D 3A 49 6E 73 |mpM:Ins
9D70: 74 61 6E 63 65 49 44 3E |tanceID>
```

# Agenda

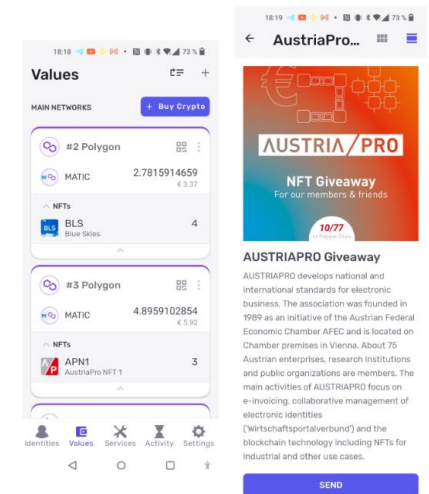
- Begrüßung
- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Themen)
- **News zum Thema NFTs**
- eDAY22 und Blockchain Award 2022
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - spontane Beiträge zu Projekten, Initiativen etc.

# Thema NFTs

- Wissenstransfer
  - Informationen und Anwendungsbeispiele:  
<https://www.wko.at/service/innovation-technologie-digitalisierung/nft-non-fungible-tokens.html>
  - Neue Expertise von AUSTRIAPRO: <https://www.wko.at/service/netzwerke/nft-als-neue-expertise-von-austriapro.html>
  - **Updates und 2 neue Dokumente in Arbeit**
- AUSTRIAPRO NFTs Serie 1
- AUSTRIAPRO NFTs Serie 2 - eDAY22
- NFTs Austrian Blockchain Award 2020-2022
  - Übermittlung erfolgt

# Wissenstransfer

- Neue Landing Page speziell für das Thema NFTs  
<https://www.wko.at/service/innovation-technologie-digitalisierung/nft-non-fungible-tokens.html>
- Setup eines Krypto-Wallets für Ethereum und ähnliche Blockchains  
<https://www.wko.at/service/innovation-technologie-digitalisierung/wallet-setup.pdf> (neuer Link)
  - Leitfaden: ibs. für „Newbies“
  - Wallet installieren/konfigurieren, Setup weiterer Blockchains
  - AustriaPro NFT Giveaway anfordern & importieren
  - ...

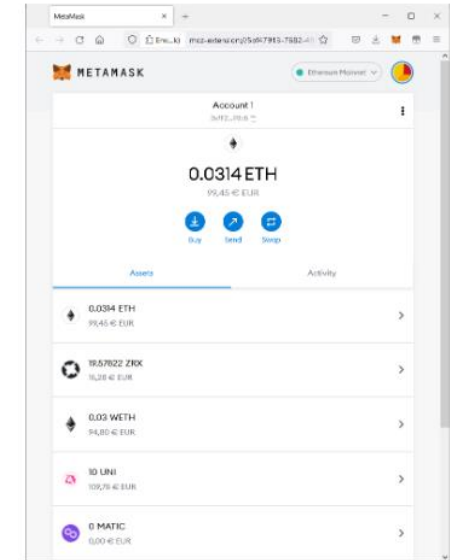
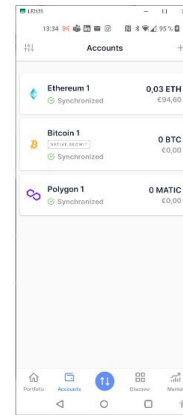


# Wissenstransfer

- Krypto-Wallets: Einleitung und Überblick  
<https://www.wko.at/service/innovation-technologie-digitalisierung/krypto-wallets.pdf> (neuer Link)

- Inhalt

- Aufgaben
  - Wofür ist es NICHT
- Funktionen
- SICHERHEIT!
- Typen
  - Softwarewallets
  - Hardwarewallets
  - „Cold Storage“
- Beispiele: Browser Plugins, Browser-Apps, Mobile Wallets, Hardware Wallets
- Betrachtung „custodial / non custodial“ Wallets

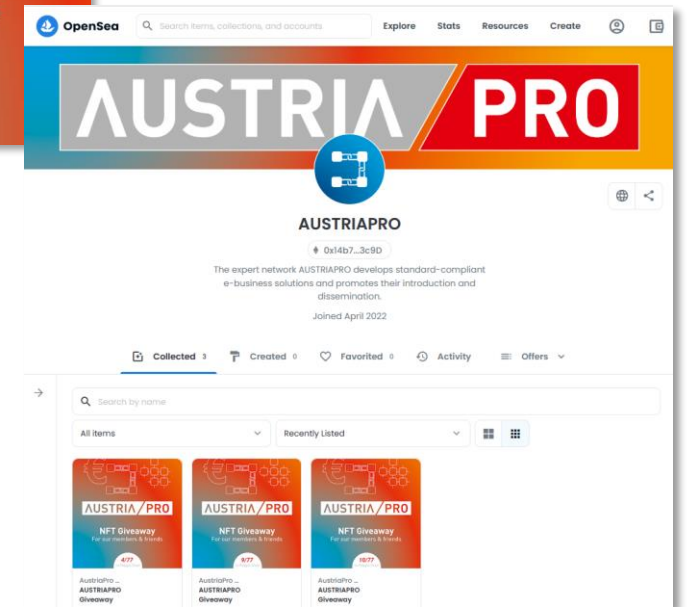
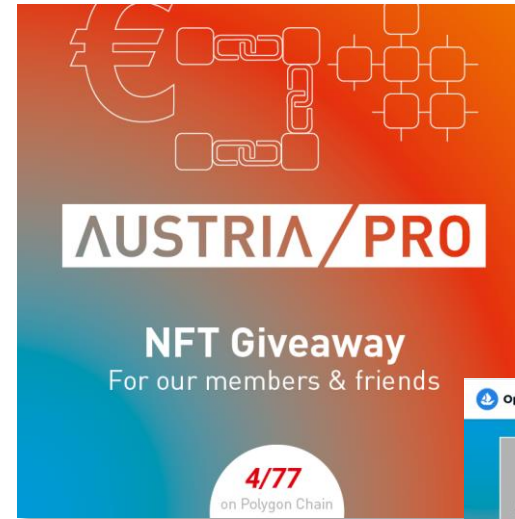


# NEWS

- Updates
  - „Setup eines Krypto-Wallets für Ethereum und ähnliche Blockchains“
- Neuer content in Vorbereitung
  - „NFTs auf OpenSea erstellen und handeln“
  - „NFTs - DIY (Do It Yourself)“

# AUSTRIAPRO NFT Give-away (Serie 1)

- Für Mitglieder & Freunde
- Limitierte Serie von 77 Stück
- Ibs. auch für „still not affine“ UserInnen
- -> Anleitung
- Auf Polygon Blockchain
  - L2-Chain auf Ethereum
  - „proof-of-stake“
  - Deutlich schneller und günstiger
- <https://opensea.io/AUSTRIAPRO>
- **Es gibt noch welche!**
  - **Wer will einen?**





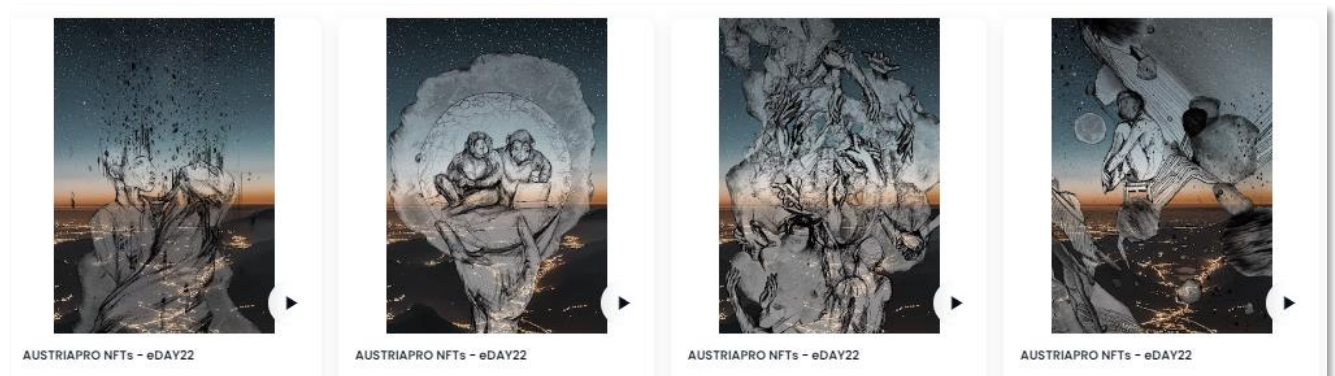
# AUSTRIAPRO NFTs (Serie 2) - eDAY22

- NFT Serie als Give-away
  - Mitglieder bzw. andere Personen, die an unseren Aktivitäten interessiert sind
- Gestaltung durch KünstlerInnen
  - 4 Illustrationen
  - 6 Hintergründe
  - 6 eigens komponierte „LoFinity“ Sounds
- $4 * 6 * 6 = 144$  Permutationen = 144 NFTs

• **Es gibt noch welche!**

• **Wer will einen?**

• [Teaser]



# Agenda

- Begrüßung
- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Themen)
- News zum Thema NFTs
- **eDAY22 und Blockchain Award 2022 - Nachlese NFTs**
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - spontane Beiträge zu Projekten, Initiativen etc.

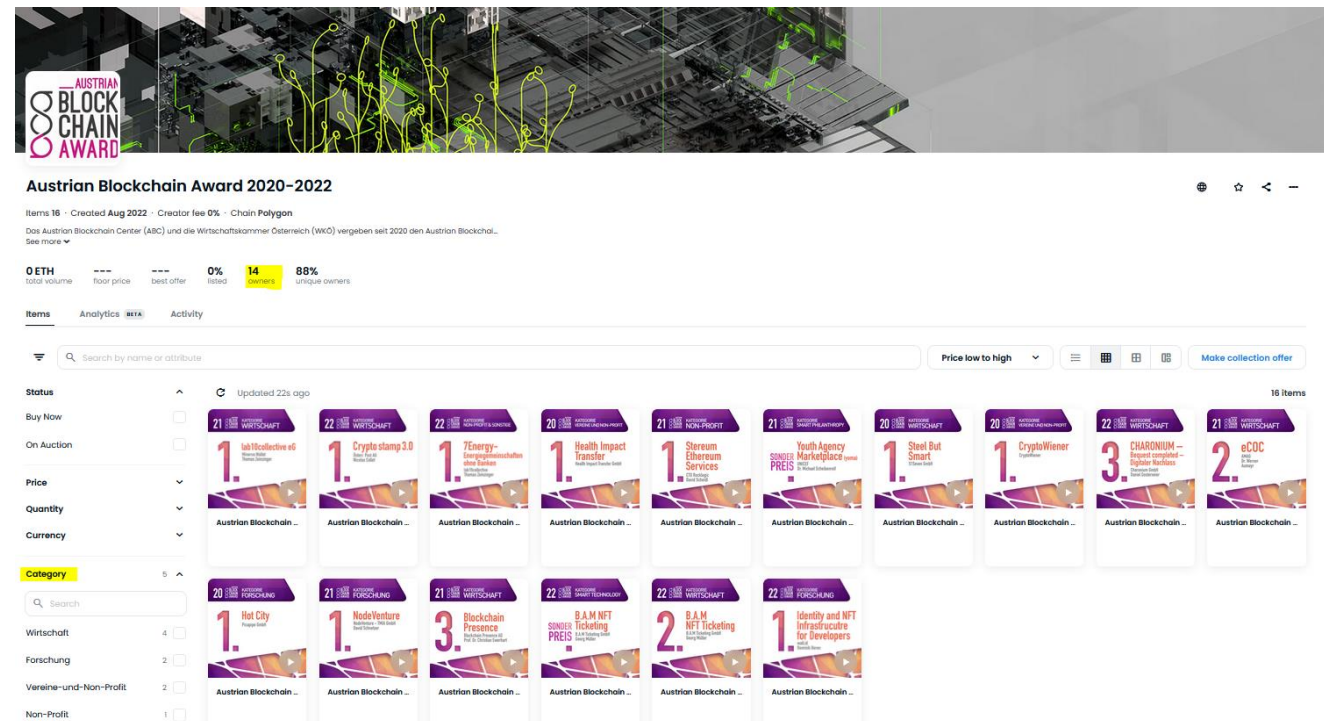
# Austrian Blockchain Award 2020-2022

- NFTs als zusätzliche Preise
  - für ehemalige und aktuelle Gewinner
- Gestaltung
  - Video mit Jingle
  - Logo
  - Infos zur Kategorie & Preisträger
- [Beispiel]



# NEWS: WKO und Austrian Blockchain Award 2020-2022

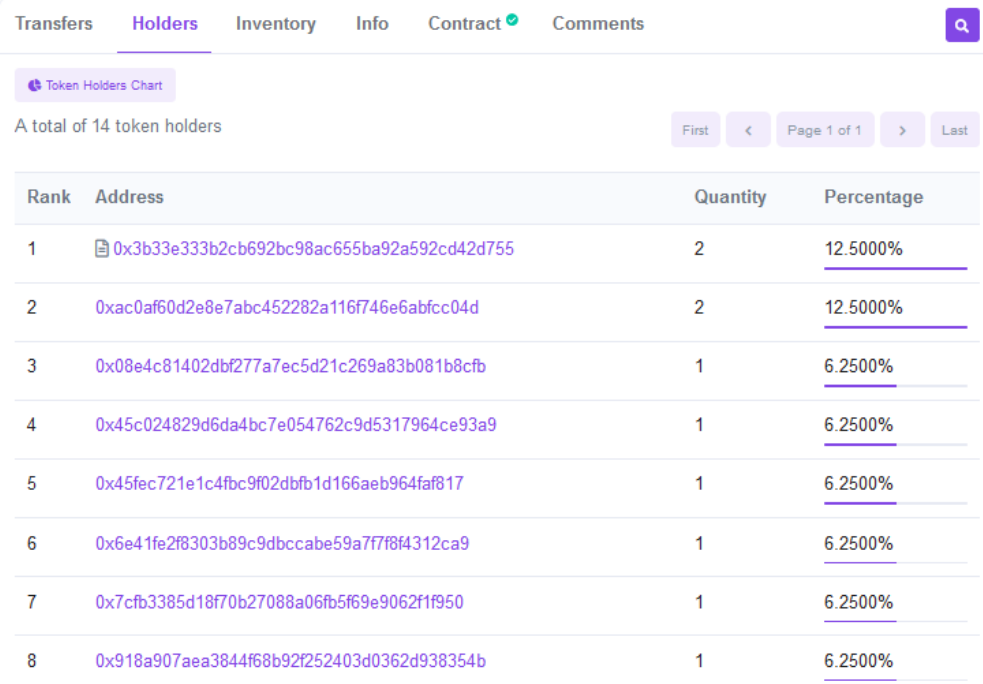
- NEWS: Die WKO hat eigenes Wallet und einen OpenSea Auftritt
- <https://opensea.io/Wirtschaftskammer>
- Collection „Austrian Blockchain Award“



The screenshot shows the OpenSea collection page for 'Austrian Blockchain Award 2020-2022'. The header features a 3D-rendered cityscape with a logo that reads 'AUSTRIAN BLOCKCHAIN AWARD'. Below the header, the collection name is displayed, along with statistics: 16 items, created in August 2022, on the Polygon chain. A summary bar shows 0 ETH total volume, 0% listed, 14 owners, and 88% unique owners. The main area displays a grid of 16 NFT items, each with a category label (e.g., 'WIRTSCHAFT', 'FORSCHUNG') and a title. A sidebar on the left provides filters for status, price, and category.

# NEWS: WKO und Austrian Blockchain Award 2020-2022

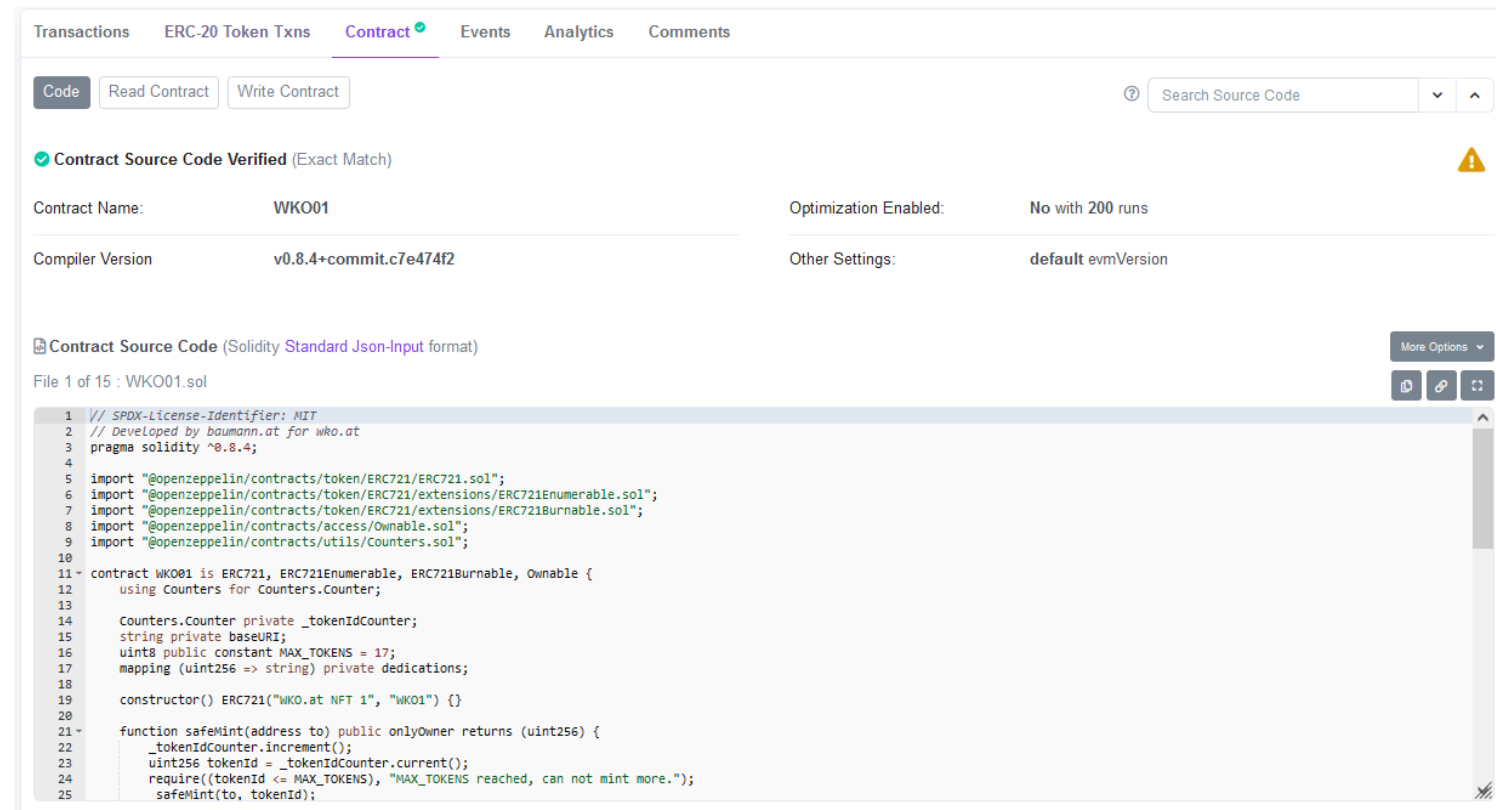
- Alle NFTs wurden den jeweiligen Preisträgern übertragen



Rank	Address	Quantity	Percentage
1	<a href="#">0x3b33e333b2cb692bc98ac655ba92a592cd42d755</a>	2	<u>12.5000%</u>
2	<a href="#">0xac0af60d2e8e7abc452282a116f746e6abfcc04d</a>	2	<u>12.5000%</u>
3	<a href="#">0x08e4c81402dbf277a7ec5d21c269a83b081b8cfb</a>	1	<u>6.2500%</u>
4	<a href="#">0x45c024829d6da4bc7e054762c9d5317964ce93a9</a>	1	<u>6.2500%</u>
5	<a href="#">0x45fec721e1c4fbc9f02dbfb1d166aeb964faf817</a>	1	<u>6.2500%</u>
6	<a href="#">0x6e41fe2f8303b89c9dbccabe59a7f7f8f4312ca9</a>	1	<u>6.2500%</u>
7	<a href="#">0x7cfb3385d18f70b27088a06fb5f69e9062f1f950</a>	1	<u>6.2500%</u>
8	<a href="#">0x918a907aea3844f68b92f252403d0362d938354b</a>	1	<u>6.2500%</u>

# WKO NFTs - Austrian Blockchain Award

- Smart Contract publiziert über Blockchain-Explorer
- <https://polygonscan.com/address/0x5400bfc0499c5ccbe5dab9db7d587cf575e51cd1#code>



The screenshot displays a blockchain explorer interface for a smart contract. At the top, there are navigation tabs: Transactions, ERC-20 Token Txns, **Contract** (selected), Events, Analytics, and Comments. Below the tabs, there are buttons for 'Code', 'Read Contract', and 'Write Contract', along with a search bar for source code. A green checkmark indicates 'Contract Source Code Verified (Exact Match)'. The contract details are as follows:

Contract Name:	WKO01	Optimization Enabled:	No with 200 runs
Compiler Version:	v0.8.4+commit.c7e474f2	Other Settings:	default evmVersion

Below the details, the contract source code is displayed in Solidity format. The code includes imports for ERC721, ERC721Enumerable, ERC721Burnable, Ownable, and Counters. The contract is named WKO01 and implements the ERC721, ERC721Enumerable, ERC721Burnable, and Ownable interfaces. It includes a constructor and a safeMint function.

```
1 // SPDX-License-Identifier: MIT
2 // Developed by baumann.at for wko.at
3 pragma solidity ^0.8.4;
4
5 import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
6 import "@openzeppelin/contracts/token/ERC721/extensions/ERC721Enumerable.sol";
7 import "@openzeppelin/contracts/token/ERC721/extensions/ERC721Burnable.sol";
8 import "@openzeppelin/contracts/access/Ownable.sol";
9 import "@openzeppelin/contracts/utils/Counters.sol";
10
11 contract WKO01 is ERC721, ERC721Enumerable, ERC721Burnable, Ownable {
12     using Counters for Counters.Counter;
13
14     Counters.Counter private _tokenIdCounter;
15     string private baseURI;
16     uint8 public constant MAX_TOKENS = 17;
17     mapping(uint256 => string) private dedications;
18
19     constructor() ERC721("WKO.at NFT 1", "WKO1") {}
20
21     function safeMint(address to) public onlyOwner returns (uint256) {
22         _tokenIdCounter.increment();
23         uint256 tokenId = _tokenIdCounter.current();
24         require((tokenId <= MAX_TOKENS), "MAX_TOKENS reached, can not mint more.");
25         safeMint(to, tokenId);
26     }
27 }
```

# Agenda

- Begrüßung
- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Themen)
- News zum Thema NFTs
- eDAY22 und Blockchain Award 2022
- **Kooperation mit DIO (Data Intelligence Offensive)**
- open space - spontane Beiträge zu Projekten, Initiativen etc.

# Kooperation mit DIO (Data Intelligence Offensive)

- ...
- Aktuelle Events: <https://www.dataintelligence.at/news-events/>



# Agenda

- Begrüßung
- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Themen)
- News zum Thema NFTs
- eDAY22 und Blockchain Award 2022
- Kooperation mit DIO (Data Intelligence Offensive)
- **open space - spontane Beiträge zu Projekten, Initiativen etc.**

## open space - Projekte, Initiativen, Informationen

- Projekt Interreg Danube Transnational Programme
  - -> Chris Boser
  - <https://www.interreg-danube.eu/>
- Vorstellung B.A.M. NFT Ticketing (Hr. Georg Müller)
- Vorstellung neues Mitglied DAAA (Hr. Holger Greiner)
- Weitere Meldungen (spontan)
- Terminavisos: Nächste AK Sitzung 24.1.2023 - 14:00



Vielen Dank für Ihre Aufmerksamkeit.

[www.austriapro.at](http://www.austriapro.at)

[austriapro@wko.at](mailto:austriapro@wko.at)

DI Dr. Christian Baumann

[c.baumann@baumann.at](mailto:c.baumann@baumann.at)

+43 664 43 24 243

