

# Blockchain Applications in AT: „Austrian Public Service Blockchain“ „Private Sector Blockchain“

Dr. Gerhard Laga, WKO

Dr. Christian Baumann, AustriaPro, Blockchain Initiative Austria

7.12.2023



AUSTRIA PRO



# Content

- Austrian Public Service Blockchain
  - Principles, Implementation
  - (Legal) Agreement
- „Proof of Existence“ - „Notarization“
- Usecases within the APSB
- Private Sector Blockchain
  - Association „Blockchain Initiative Austria“
  - Landscape, Artifacts, „Dual Verify“
- APSB & PSBC - comparison
- Summary

# Austrian Public Service Blockchain

- Initiative of public administration institutions
  - “Consortium blockchain” for different use cases in the “public service” area
  - Blockchain in real operation since 10/2019
- Consortium partner currently
  - WKO (Chamber of Commerce): Data certification
  - WU (Vienna University of Economics and Business): Data certification
  - City of Vienna: OGD notarization
  - BRZ (Federal Computing Center)
  - Nic.at (cert.at)
  - Ministry of Health (BMSGPK)
  - OeKB (Austrian Control Bank) (committed)
  - Requested
    - St. Pölten University of Applied Sciences
    - Vienna University of Technology...

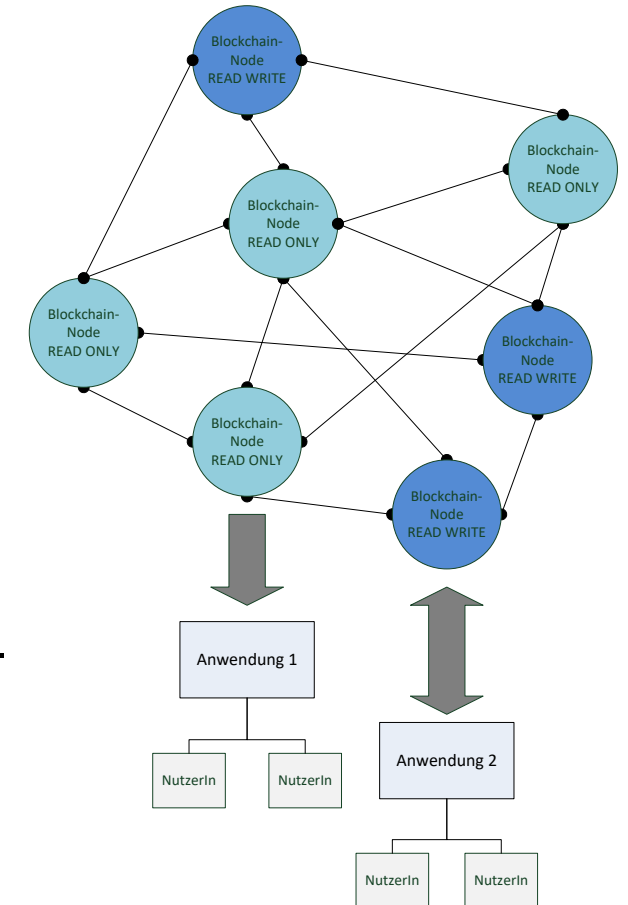
Austrian Public Service Blockchain (Nodes)	Test	Produktiv
BRZ (Bundesrechenzentrum)	ja (2)	ja (2)
Stadt Wien - MA01	ja (2)	ja (2)
WKO (Wirtschaftskammer Österreich)	ja	ja
nic.at/cert.at	ja	ja
WU (Wirtschaftsuniversität Wien)	ja	ja
BMSGPK (Gesundheitsministerium)		ja
AUSTRIAPRO	(ja)	
<b>Summe</b>		<b>8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

# APSB Principles

- The consensus algorithms used ensure that no **energy-wasting mining** is carried out and that the infrastructure is designed to be environmentally friendly and resource-friendly
- **Made in Austria**, but under observation of EU activities (EBSI)
- Application of **open source** software
- **Data protection (GDPR)**: Personal data is stored offchain and is not the subject of these infrastructures.

# APSB Implementation

- Based on “MultiChain”
  - Opensource (multichain.com)
  - Extensive configuration options and security mechanisms
- Configuration as a “consortium chain”
  - Write access only for known (authenticated) participants
  - Public read access possible
  - Consensus algorithm: “Proof of Authority”
  - This means NO (unnecessarily) high energy requirements - such as at “Proof of Work”



# APSB Agreement



- Agreement is available in version 1.0
- Attachments
  - Template for joining the APSB
  - Technical Specification (Implementation Guide)
    - Requirements server, VPN, multichain environment, data structure...
  - APSB presentation materials for management
- Status
  - Approved by BLSG (Fall 2022)
  - Publish on e-Government Reference Server as a “recommendation” - ongoing
  - <http://reference.e-government.gv.at>
  - <https://neu.ref.wien.gv.at/>

## 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

# „Proof Of Existence“

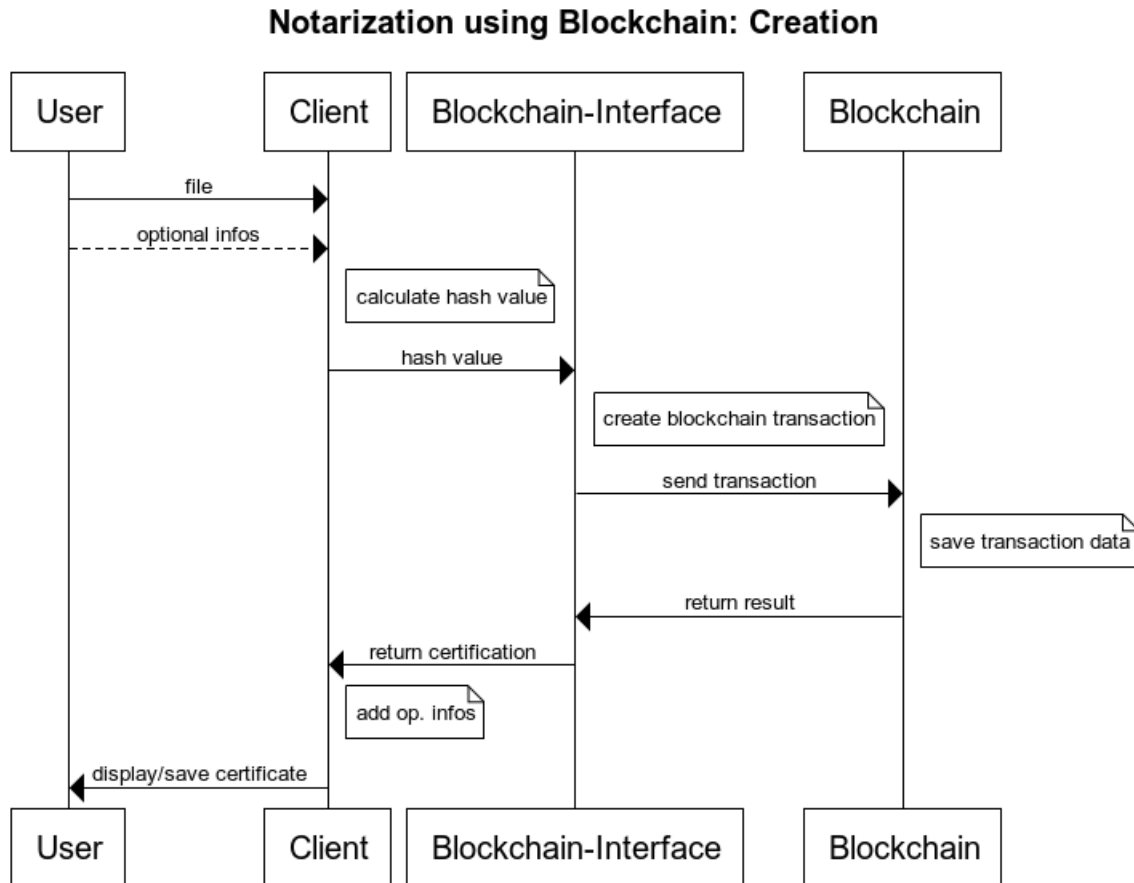
- Problem
  - Electronic documents are easy to copy & change, i.e. manipulate.
  - Proof of authenticity in the real world is time-consuming & expensive
  - Even "digital signature" only partially solves problem
- Blockchain technology as a solution?
  - Hash value (digital fingerprint) proves content
  - Block time proves timestamp
  - Blockchain ensures immutability

# „Proof Of Existence“ - „Notarization“

- Notarization can be used to prove that an
  - electronic document
  - existed at a certain point in time
  - in a certain form and
  - has not been changed since then.
- The security and trust that
  - notarized data cannot be manipulated
  - are guaranteed by blockchain technology
- Only anonymous data is processed!
  - i.e. hash values of electronic documents
  - in any case NO personal data (GDPR relevant)



# Process - Creation



- Hash value is created on client
- I.e. files stay in sphere of the user
- Additional infos (Filename, Comments) are for reference only and NOT stored on the blockchain

# Notarization - Verification (Example: Web-GUI)

The screenshot displays the proof.li web-GUI. On the left, the 'Create notarization' form is visible, showing the document 'Meeting\_CP132\_20220404.pdf' with a calculated hash value of 5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6. The form includes fields for filename and remark, and a 'Create' button. On the right, the 'Result of the creation' section shows a green checkmark and the message 'Notarization created.' Below this, a table lists the details of the notarization, including the time stamp, hash value, transaction-ID, filename, and remark. A QR code is provided for verification, and a link to the verification page is shown at the bottom right.

**Result of the creation**

Notarization created.

The notarization was created successfully, details are shown in the following bottom of page).

<b>Time stamp</b>	2022-04-12T10:29:50+02:00
<b>Hash value</b>	5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6
<b>Transaction-ID</b>	5e3ec1ff4d390138efec0bbc7f0fe0371cd32a6963b1
<b>Filename (*)</b>	Meeting_CP132_20220404.pdf
<b>Remark (*)</b>	Report Meeting CP132

(\*) for reference, will NOT be stored in the blockchain.

**Document Notarization - Certificate**

**Created at 12.04.2022 - 10:35:20**


This is to certify, that the hash value ("SHA256") of the document was securely and immutably stored in the blockchain.

The following table shows all details:

Time stamp	2022-04-12T10:35:20+02:00
Hash value	5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6
Transaktions-ID	af282475078ca66e6f42dfdbb19850003ea8584d4205c961ac8e30c8f3471f04
Filename (*)	Meeting_CP132_20220404.pdf
Remark (*)	Report Meeting CP132

Data marked with (\*) is for information and reference only and not stored in the blockchain.

By using the following QR-Code or link you can invoke a verification service and pass the hash value.

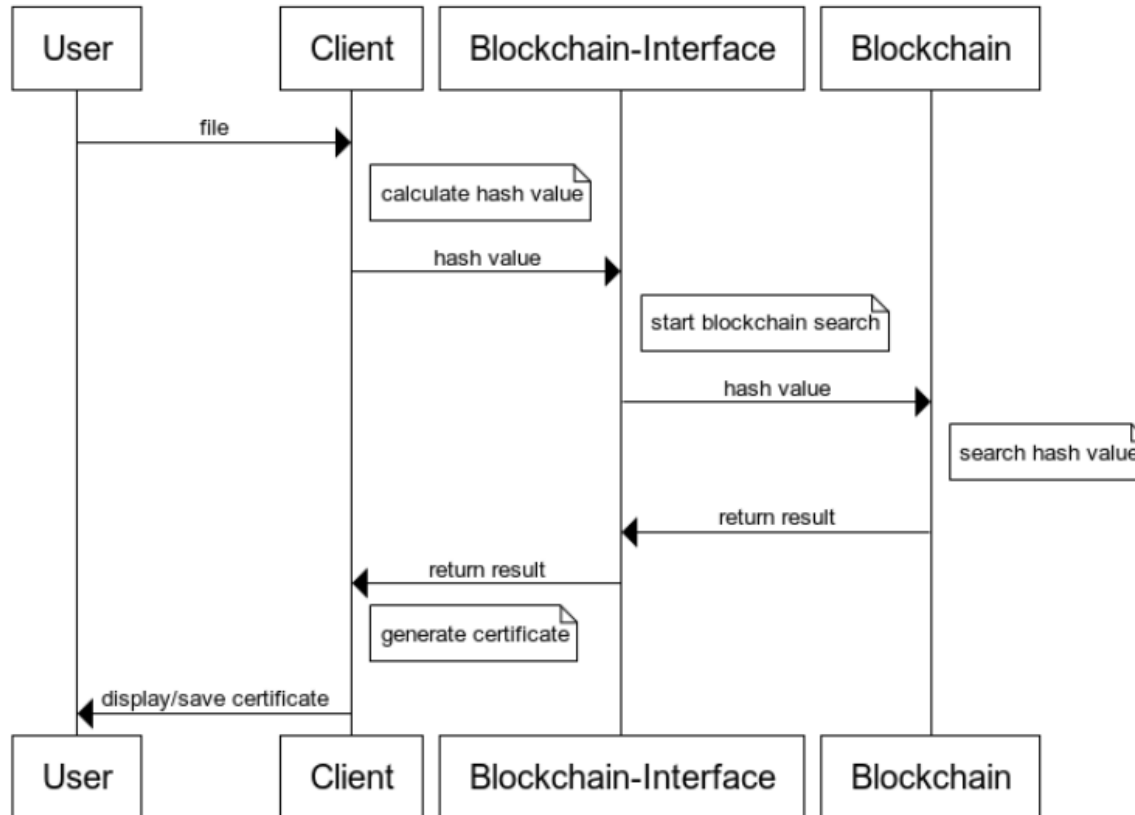


<https://proof.li/?page=verify&fileHash=5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6>

Example „proof.li“ operated by <https://bc-init.at>

# Process - Verification

## Notarization using Blockchain: Verification



## Possible Results

- NO Match: „This document was not notarized using this system“
- ONE Match: „This document was notarized at [TimeStamp]“
- MORE Matches: „Oldest entry is relevant.“

# Notarization - Verification (Example: Web-GUI)

## Verify notarization

Here you can check whether/when a document was notarized, i.e. the digital fingerprint (hash value) of a file was stored in the blockchain.

To do this, select the corresponding file (the hash value is calculated automatically), or enter

Select file (will NOT be uploaded to the server) to calculate hash value:

Meeting\_CP132\_20220404.pdf

or hash value (sha256):

or Transaction-ID:

The entered data is searched in the blockchain and displayed accordingly.

## Result of the verification



Hash value "5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6" found.

One entry was found, i.e. the document with the corresponding hash value was notarized in this system at the specified time.

## Record 1/1

<b>Block hash</b>	0056149bdabd6f8635ca8393f7130aea9ac5d0728f0c0c42f3bf8f7a3097996b
<b>Block time</b>	2022-04-12T10:30:06+02:00
<b>Confirmations</b>	14
<b>Time stamp</b>	2022-04-12T10:29:50+02:00
<b>Hash value (sha256)</b>	5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6
<b>Transaction-ID</b>	5e3ec1ff4d390138efec0bbcf7f0fe0371cd32a6963bb909a5742d578b209441

# Notarization - possible areas of application

- Indisputable evidence of **business correspondence**
  - Draft contracts, supply agreements, invoices ...
- Protection of **intellectual property**
  - Concepts, texts, graphics, photos, film, software ...
- Long-term evidence of data from the **production process**
  - Batches, serial numbers, temperature curves, function tests on machines ...
- Traceable data for **transport & logistics** (supply chain)
- All kinds of **certificates**, attestations, confirmations ...

# Usecases within the APSB

- WKO - „Data Certification“
- Vienna - „OGD Notarization“
- WU Wien (University of Economics) - Academic integrity & certificates
- BMSGPK (Ministry of Health) - health data

# „Data Certification“ („Daten-Zertifizierung“)

- Alternative term for “notarization” coined by WKO
- A digital service for
  - WKO members
  - and internal use
- Real operation since 11/2019
  - As part of the “Austrian Public Service Blockchain”

## Blockchain-Service Datenzertifizierung

Innovationsservice: Daten einfach, sicher und kostenlos digital zertifizieren



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.

Auf [Mein WKO](#) ist das Blockchain-Datenzertifizierungsservice für Mitglieder der Wirtschaftskammern Österreichs kostenlos verfügbar.

# WKO „Daten-Zertifizierung“ - Datei zertifizieren



Blockchain Datenzertifizierung

**Erstellen**      Überprüfen

Datei auswählen

Anmerkung...  
0 / 150

Jetzt Bestätigung erstellen

Blockchain Datenzertifizierung

**Erstellen**      Überprüfen

Dokumentation\_Nachträgliches\_Ubermitte... ✕

Version 2.1, CB|  
15 / 150

Jetzt Bestätigung erstellen

Blockchain Datenzertifizierung

✓ Dokumentation\_Nachträgliches\_Ubermit...

Erstellt am 08.09.2021 12:16

Anmerkung  
Version 2.1, CB

Transaktions ID

618d504cc592954eaefe3490c9c2304

Zurück      Bestätigung öffnen

<https://mein.wko.at>



# WKO „Daten-Zertifizierung“ - Bestätigung



## Blockchain Datenzertifizierung - Bestätigung

Erstellt am 08.09.2021 um 12:16:41 Uhr

Zum angegebenen Zeitpunkt wurde der digitale Fingerabdruck (Hashwert) der Datei in der [Blockchain](#) hinterlegt.

Details zur hinterlegten Datei:

Dateiname	Dokumentation_Nachträgliches_Übermitteln_von_Datenfeldern_zu_bereits_übermittelten_Labormeldungen_HL7-Schnittstelle.pdf
Digitaler Fingerabdruck (Hashwert)	36d965ff34729bc51a968fc018e41bca7ba11763211d83a047d0845d4c3b08a2
Anmerkung beim Einbringen	Version 2.1, CB
Transaktions-ID zur direkten Verifizierung in der <a href="#">Blockchain</a>	618d504cc592954eae3490c9c23047daa7e9483df02722b611a81a7bc9e3dd

Bitte speichern Sie diese Bestätigung gemeinsam mit einer Kopie der soeben zertifizierten Datei ab. Sie können dann mit dem Original weiterarbeiten, sofern Sie dies wünschen.

Die Kopie der zertifizierten Datei sollte nur über den Dateimanager kopiert bzw. verschoben und nicht geöffnet und neu abgespeichert werden, da sich sonst der digitale Fingerabdruck verändern kann.

Sollten Sie doch die Datei abgespeichert haben, bringen sie diese einfach erneut ins Datenzertifizierungsservice ein.

Der unten angeführte QR-Code erleichtert ihnen das Aufrufen des Überprüfungsservice. Er enthält eine URL der soeben generierten Transaktion und kann mit einem Smartphone und einer QR-Reader-Software ausgelesen werden. Sie können die Transaktions-ID zur direkten Verifizierung in der [Blockchain](#) mit folgendem QR-Code bzw. Link an ein Verifikationsservice übergeben.



<https://daten-zertifizierung.at/verify?txid=618d504cc592954eae3490c9c23047daa7e9483df02722b611a81a7bc9e3dd>

### Neue Nachrichten

Suchbegriff...

Blockchain Datenzertifizierung	Persönlich	Erledigt	heute		
Blockchain Datenzertifizierung	Persönlich	Erledigt	17.05.2021		
Blockchain Datenzertifizierung	Persönlich	Erledigt	24.04.2021		
Blockchain Datenzertifizierung	Persönlich	Erledigt	14.04.2021		

#### Nachricht 1069490

### Blockchain Datenzertifizierung

beantragt für: Persönlich  
Status: Erledigt  
letzte Änderung: 08.09.2021 um 12:16 Uhr

Guten Tag,

die Bestätigung des Dokuments "Dokumentation\_Nachträgliches\_Übermitteln\_von\_Datenfeldern\_zu\_bereits\_übermittelten\_Labormeldungen\_HL7-Schnittstelle.pdf" steht unter folgendem Link zum Download bereit.

Freundliche Grüße  
Ihre Wirtschaftskammern Österreichs

Bestätigung: <https://edocument.wko.at/download/file/6d447699-0f5d-4a6d-8df5-61cbd6500980>

[schließen](#)

# WKO „Daten-Zertifizierung“ - Verifikation

The screenshot displays the 'Blockchain Datenzertifizierung' application interface. It is divided into three main sections: a creation form, a document overview, and a detailed verification view.

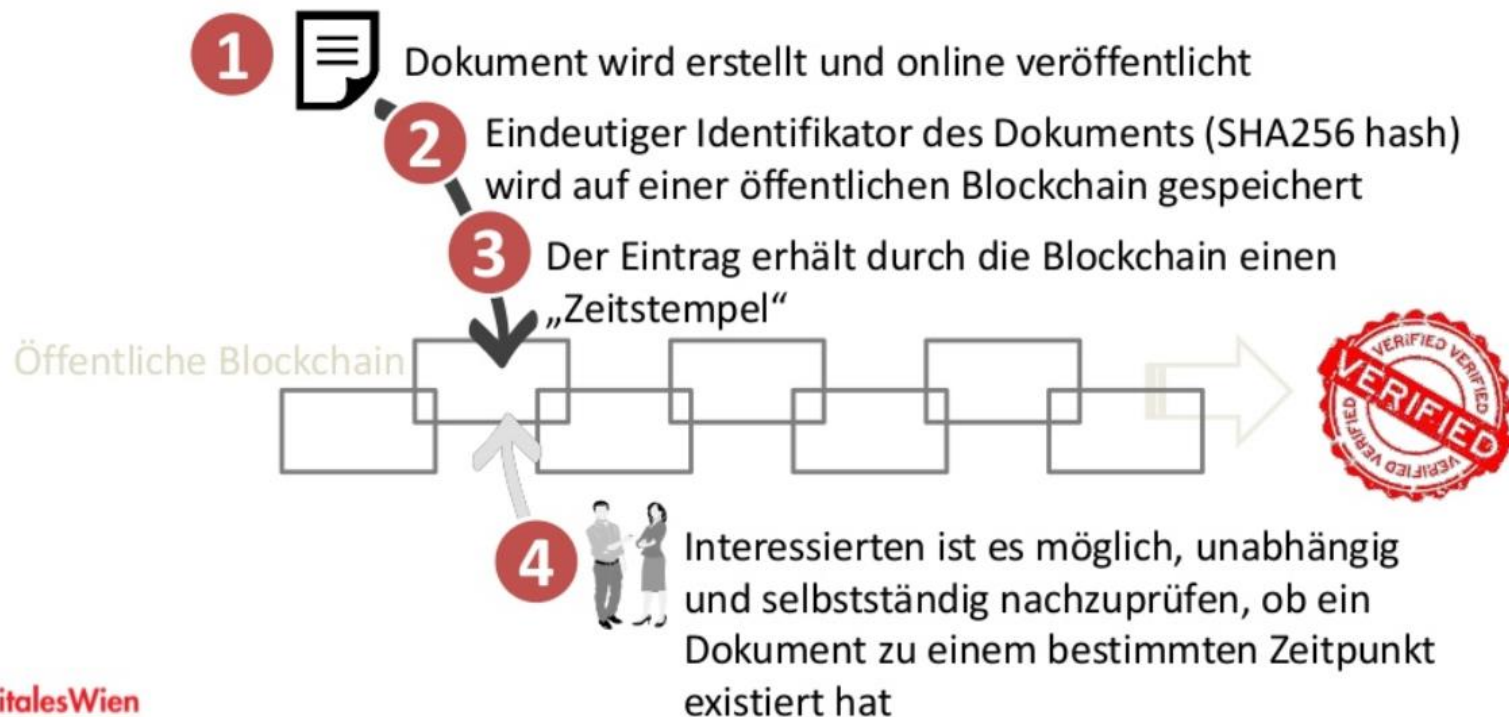
**Creation Form (Left):** Features a '+ Erstellen' button, a search icon, and a document title 'Dokumentation\_Nachträgliches\_Ub'. It contains input fields for a hash ('36d965ff34729bc51a968fc018e4...') and an optional transaction ID. A red-bordered button at the bottom reads 'Jetzt Dokument überprüfen'.

**Document Overview (Middle):** Shows a document titled 'Dokumentation\_Nachträgliches\_Ub' with a green checkmark. It lists the creation date as '08.09.21' and the digital fingerprint (hash) as '36d965ff34729bc51a968fc018e41bca7ba11763211d83a047d0845d4c3b08a2'. The transaction ID is '618d504cc592954eaefe3490c9c23047daa7e9483df02722b611a81a7bc9e3dd'. Navigation buttons 'Zurück' and 'Details ansehen' are visible.

**Details View (Right):** Titled 'Details zum Dokument', it provides a detailed explanation: 'Der digitale Fingerabdruck (Hashwert) wurde in der Blockchain gefunden und zum ersten Mal am 08.09.2021 eingebracht.' It repeats the hash and transaction ID values. A concluding statement reads: 'Damit ist bewiesen, dass das Dokument mit diesem Fingerabdruck seit dem Einbringen in das Datenzertifizierungsservice nicht verändert wurde.' The creation timestamp is '08.09.2021 12:16'.

# „Notarisierung in Wien“

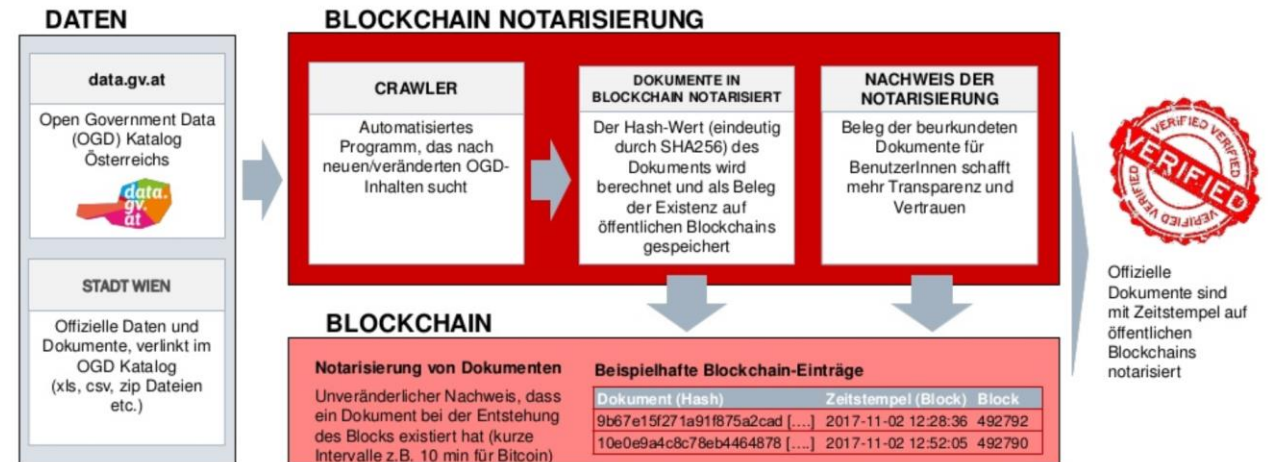
Die Blockchain ermöglicht nachvollziehbare, öffentliche Nachweise ohne zentrale Autorität



# APSB - Wien - OGD Notarization

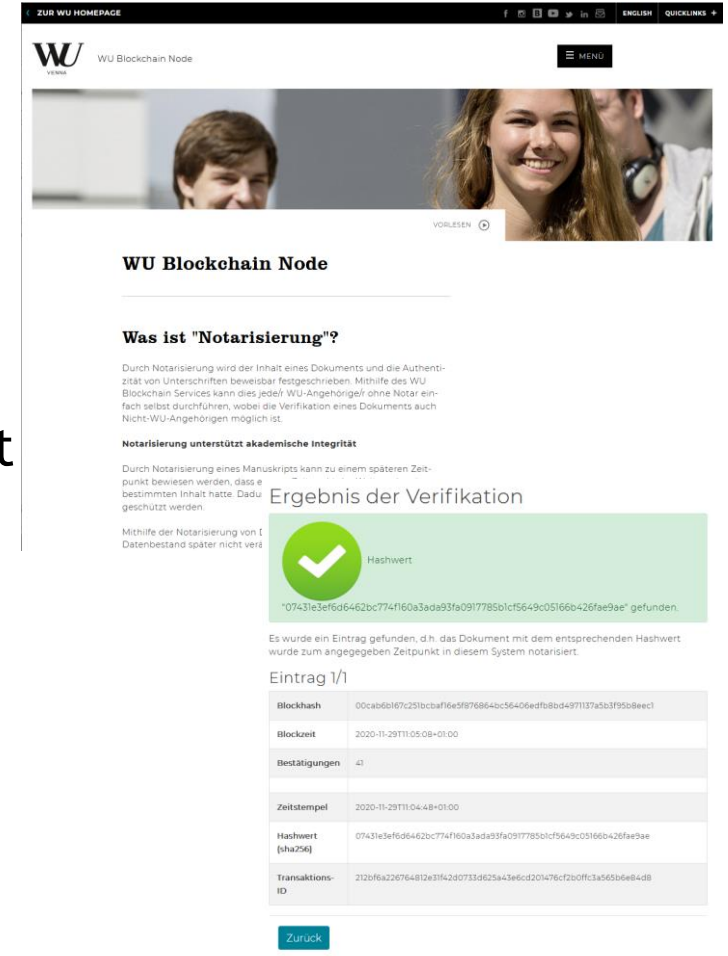
Securing the integrity of open government data through hash values in a blockchain

- Dec. 2017: 1st blockchain pilot
- Current project: Conversion of the blockchain infrastructure to APSB
- Planned real operation in 2024



# APSB - WU (Vienna University of Economics and Business)

- In operation since 12/2020
- Use case 1: notarization - academic integrity
  - Manuscripts - copyright of the author
  - Data - data base not changed (no adapting empirical surveys to hypotheses)
  - References, confirmations and certificates (even without an official signature)
- Organizational framework
  - Create notarizations - only from WU's internal network (or VPN)
  - Verify notarizations - also from a public network - and via Dual-Verify



The screenshot shows the WU Blockchain Node website. The header includes the WU logo and navigation links. The main content area features a section titled "WU Blockchain Node" and a sub-section "Was ist 'Notarisierung'?" which explains the process of notarization. Below this, there is a section for "Ergebnis der Verifikation" (Verification Result) showing a green checkmark and a hash value: "07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c05166b426fae9ae" gefunden. A table below the verification result displays the following data:

Blockhash	00cab6b187c231bcbaf16e5f876864bc56406edf8bd497137a3b3f95b8ec1
Blockzeit	2020-11-29T11:05:08+01:00
Bestätigungen	1
Zeitstempel	2020-11-29T11:04:48+01:00
Hashwert (sha256)	07431e3ef6d6462bc774f160a3ada93fa0917785b1cf5649c05166b426fae9ae
Transaktions-ID	212bfe226764812e31a2d0713d625a43e6cc201476cf2b0ffc3a565b6e4d8

A "Zurück" button is located at the bottom of the page.

# Absicherung der SAP Zertifikate



Prof. Dr. Alfred Taudes



# Use case 2: SAP Certificates

- Addition to the certificate for the WU SAP-based course in production and supply chain management
- Traditional paper certificates issued together with SAP Austria since the 90s
- Now a quality feature that students like to use for applications => high level of awareness in AT



Institute for Production Management

**CERTIFICATE**

Mrs./Mr.

Student ID:

passed the following SAP-based teaching program in S/W semester Jahr:

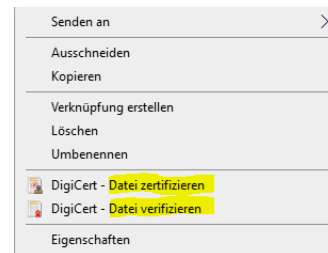
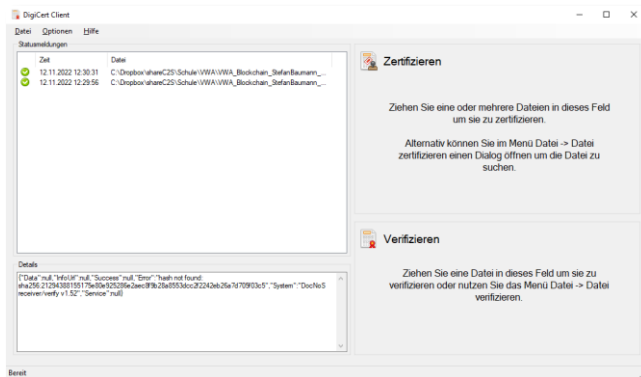
- Datawarehouse Management with SAP BW: An Introduction to Business Intelligence
- Datawarehouse Management with SAP BW: An Introduction
- Integration Management with SAP ECC: An Introduction to Controlling and Logistics
- Integration Management with SAP ECC: Implementation Project
- Integration Management with SAP ECC: Implementation Project II
- Datawarehouse Management with SAP BW: Balanced Scorecards
- Integration Management mit SAP APO (Vertiefung)
- Enterprise Resource Planning Systems (ERP-Systems)
- Project Management with SAP
- Business Analytics in Supply Chains 1 (BA 1)
- Business Analytics in Supply Chains 2 (BA 2)

Christina Wilfinger, SAP Österreich

ao.Univ.Prof. Dr. Alexander Prosser

# SAP Certificates - How does it work?

- Option 1: Web-GUI (see previous slides)
  - Ideal for single/few notarizations
- Option 2: Windows-Client
  - Integration in Office-Workflow
  - Batch notarization possible
  - Automatic generation/download of „notarization infos“ as PDF



## Datenzertifizierung - Zertifikat

Erstellt am/um 31.03.2022 - 14:34:52

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

Details zum hinterlegten Dokument:

Zeitstempel	2022-03-31T14:34:52+02:00
Hashwert	42d60663f7999437219473d44d1988c114cbf6ec1c67ec66f8cd5e3ff395cf78
Transaktions-ID	3ae6c42c2aa0f98911dab85dc8e1e57db63d7f2100f3756b7577272db227437e
Dateiname (*)	
Anmerkung (*)	

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://www.wu.ac.at/blockchain/verify/?fileHash=42d60663f7999437219473d44d1988c114cbf6ec1c67ec66f8cd5e3ff395cf78>

Weitere Informationen siehe <https://www.wu.ac.at/blockchain/>



# SAP Certificates - Acceptance

- In use since summer semester 2021
- Since then, around 400 certificates issued
- Students increasingly requested notarized certificates, especially in the summer semester of 2023, and used them, for example, for applications for semesters abroad


# Deployment in the Ministry of Health (BMSGPK)

- The BMSGPK has been operating a blockchain node as part of the “Austrian Public Service Blockchain” since 6/2022.
- The first application “Data Certification for OpenData” has been running since August 2022.
- Data from the Covid19 and vaccination dashboards are certified (notarized).
- Further applications are being planned.
- The BMSGPK also operates a publicly accessible verification service.
- BMSGPK Node will probably also be used by AGES (currently in test operation), documents from the health sector (OpenData)

# Example: Certified data “vaccination dashboard”

<https://info.gesundheitsministerium.at/opendata>

Dashboard is currently offline: Revision due to the new vaccination recommendations

 Corona in Österreich   Impfzahlen   Fall- und Testzahlen

## Open Data

### Veröffentlichte Datensätze

#### COVID-19 Impfungen

- **Verabreichte Impfungen als Zeitreihe, nach Bundesländern, Impfstoff und Dosiszahl**
- **Verabreichte Impfungen in demografischen Gruppen**
- **Laut den NIG-Empfehlungen geimpfte Personen in demografischen Gruppen**
- **Laut den NIG-Empfehlungen geimpfte Personen und verabreichte Impfungen pro**

#### Gemeinde

- **Bestellte und ausgelieferte Impfungen aus dem e-Shop der BBG**

#### COVID-19 Fallzahlen

- **Bestätigte Fälle laut EMS**
- **Zahlen laut Bundesländermeldungen an den nationalen Krisenstab**

#### COVID-19 Testungen

- **Gemeldete Tests von Apotheken und Betrieben**




The screenshot shows the 'data.gv.at' website interface. The main heading is 'Katalog COVID-19: Zeitreihe der verabreichten Impfdosen der Corona-Schutzimpfung'. Below this, there is a description of the dataset: 'Die Zeitreihe der verabreichten Impfdosen der Corona-Schutzimpfung, aufgeteilt nach Hersteller, Dosisnummer (1, 2, 3, 4, 5+) und Bundesländern. Wird einmal täglich aus dem System des e-Impfpass aktualisiert.' To the right, there are filters for 'Veröffentlichende Organisation bzw. Person' (BMSGPK) and 'Kategorie' (Gesundheit). Below the description, there are buttons for 'Mehr Information' and 'Zur Ressource'. A table below lists details for the dataset 'COVID19\_vaccination\_doses\_timeline\_v202206.csv':

Titel und Beschreibung	Timeline of administered COVID-19 vaccination doses
Englisch	
Datenverantwortliche Stelle	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
Kontaktseite der datenverantwortlichen Stelle	<a href="https://www.sozialministerium.at/Ministerium/Kontakt.html">https://www.sozialministerium.at/Ministerium/Kontakt.html</a>
Datenverantwortliche Stelle - E-Mailkontakt	opendata@sozialministerium.at

On the right side of the table, there are 'Schlagworte' (tags) including COVID, COVID-19, Corona, Epidemie, Gesundheit, Krankheit, NIG, Nationales Impfgremium, Pandemie, Schutzimpfung, Tests, Testungen, and Virus.

# Verification-Service of the BMSGPK

 **Bundesministerium**  
Soziales, Gesundheit, Pflege  
und Konsumentenschutz

Blockchain-Service Daten-Zertifizierung

## 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 im Blockchain-System **Austrian Public Service Blockchain** (aka "Blockstempel") 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... **COVID19\_vaccination\_doses\_timeline\_v202206.csv**

Digitaler Fingerabdruck (Hashwert sha256)

**bf65a4f8d5fd217f7378610ea538187914aaed589ed82cf256b7b6abc5613ebb**

Alternativ Transaktions-ID eingeben:

Optional: Alle Details anzeigen

**Dokument verifizieren**

## Ergebnis der Überprüfung

Es wurde im Blockchain-System **Austrian Public Service Blockchain** (aka "Blockstempel") gesucht.

## Zusammenfassung



Hashwert "bf65a4f8d5fd217f7378610ea538187914aaed589ed82cf256b7b6abc5613ebb" 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

<b>Zeitstempel</b>	<b>2022-09-05T09:17:29+02:00</b>
<b>Transaktions-ID</b>	320292b5fd8ca0f3594624dc801a30db4d1479fc4f0478699dd3d2581b0a250f
<b>Hashwert (sha256)</b>	<b>bf65a4f8d5fd217f7378610ea538187914aaed589ed82cf256b7b6abc5613ebb</b>
<b>Blockzeit</b>	2022-09-05T09:17:35+02:00
<b>Blockhash</b>	00c837ef65f6ca92ea4ec0163db10c707d140bcced4d2943f5b5d34232fb4d34
<b>Bestätigungen</b>	157

**Zurück**

# Notarization for software artifacts

- Prototype status
- Java Development
- Local gitlab environment
- Notarizing script in build pipeline
  - calculates hash values of artifacts
  - calls DocNoS-API
  - notarizes the artifacts (\*.war, \*.jar)

<b>Publishers</b>	13VXwdarLRtV5fyP8qdWEFxebe6Ay45pgdY4Bb
<b>Key 0</b>	<a href="#">id:183eb60f-ec79-4d8a-9f18-50bf5a22fc43</a>
<b>Key 1</b>	<a href="#">sha256:41730b0b59b99db62491d76ded4399595b18bb70e4839dd10726e942109cd262</a>
<b>Key 2</b>	<a href="#">sha512:edf1fb634518fa7964b19e9cc02f497c82200e019765126af7605fb74444846e05c9395a29c3a9e14f4f9655b3dc0</a>
<b>Key 3</b>	artino/Test
<b>JSON data</b>	<pre>{   "timeStamp": "2023-12-04T12:39:45+01:00",   "client": "artino/Test",   "version": "DocNoS-v1.1",   "data": {     "id": "183eb60f-ec79-4d8a-9f18-50bf5a22fc43",     "hashes": {       "sha256": "41730b0b59b99db62491d76ded4399595b18bb70e4839dd10726e942109cd262",       "sha512": "edf1fb634518fa7964b19e9cc02f497c82200e019765126af7605fb74444846e05c9395a29c3a9e14f4f9655b3dc0"     },     "remarks": "artifact openatna-web-7.0.0.war notarized by gitlab"   } }</pre>

# „Private Sector Blockchain“

- „AUSTRIAPRO“
  - Standardization and expert platform in collaboration with WKO
  - WG Blockchain, Blockchain-Lab
- Initiative "Private Sector Blockchain"
- Goals
  - Consortium blockchain for data certification
  - Building a permanent and secure blockchain infrastructure for Austria's economy
  - Establishment and moderation of an open stakeholder forum to set up and manage the infrastructure
- -> Recommendation from project with Austrian Blockchain Center (2020)
- -> Association „Blockchain Initiative Austria“

# BCI

Blockchain Initiative Austria

- Blockchain Initiative Austria
  - Founded 1/2021
- Currently (12/2023)
  - 22 Members & 1 Network partner (DLT Austria)
- <https://www.bc-init.at/>
  - Member list
  - Association statutes
  - Application for membership
  - System description & framework conditions
  - Specifications...



## Aktuelle Mitgliederliste

ABC Research GmbH - Austrian Blockchain Center	
Agordanza Einmangeldiamanten Handels GmbH	
AUSTRIAPRO - Verein zur Förderung standardkonformer e-Business Lösungen	
baumann - Blockchain Consulting & Development	
Bridge of Trust - digital	
DEUDAT GmbH - Datenschutz und Informationssicherheit - Anwendung: Notariatslösung	
docnodes gmbh - Dokumenten/Notariatslösung auf der DeVoS Blockchain	
Infinite Trust Digital GmbH	
IoT Austria - The Austrian Internet of Things Network	
IVM Technical Consultants GmbH	
Kosch & Partner Rechtsanwälte GmbH Anwendung: Digitale Zertifizierung	
MC TechAdvisors GmbH	
RBK - Digging, Roman Brudberger-Koch	
SEC Consult Unternehmensberatung GmbH - Anwendung: ForensicForewar	
sekdigital - (in Vorbereitung)	
Securikett Ulrich & Horn GmbH	
SIMTOOLS GmbH	
SYNERCON GmbH	
VIM Internetaustauschlösungen GmbH	
Woschitz group GmbH	

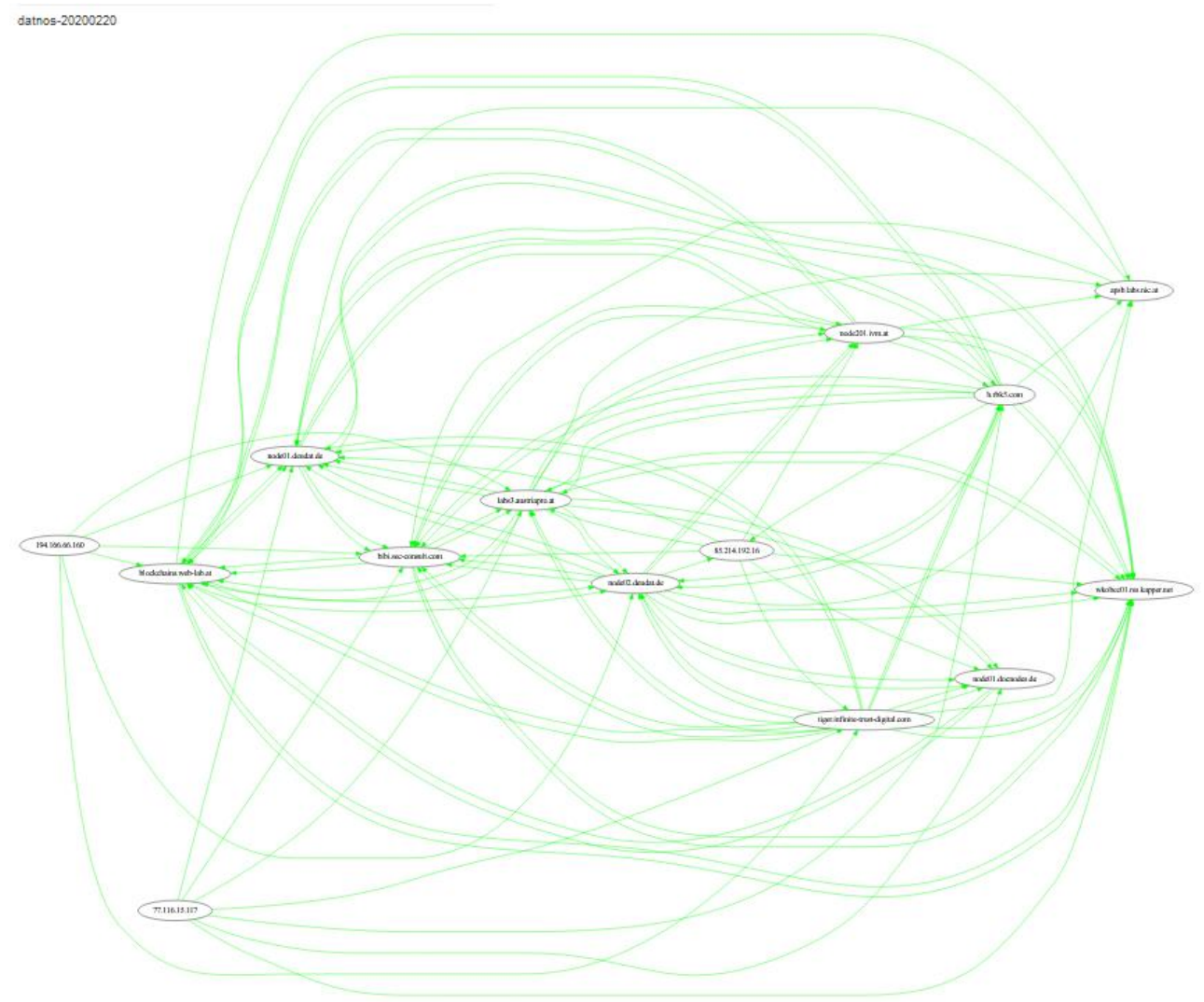
## Ehrenmitglieder

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

INTERDISCIPLINARY RESEARCH INSTITUTE FOR CRYPTOECONOMICS

# Infrastructure

- Blockchain in productive operation since 20.2.2020
  - Currently 14 nodes
- First use case: “Data certification”
- Multiple applications in real operation
- So far (12/2023) approx.
  - 500,000 blocks
  - 450,000 transactions
- <https://www.bc-init.at/blockchain>





## Usecases PSBC - selected examples

- Data certification
  - multiple applications (members)
- blockchain-dataroom.de
  - new files (version) uploaded to dataroom are automatically notarized
- Death certificates from crematoriums
  - largest crematorium in Germany
  - official medical examination („amtsärztliche Leichenschau“) digitized and notarized (approx. 5000/month)

# Legal: Private expert opinion on “notarization” (Privatgutachterliche Stellungnahme zu „Notarisierung“)

## Privatgutachterliche Stellungnahme

### Report

- Analogous to report (APSB - AustriaPro/WKO)
- Focus „Private Sector Blockchain“
- Framework conditions for the setup and operation of the consortium blockchain operated by the association members

[https://www.bc-init.at/files/Gutachten\\_Dokumenten-Notarisierung\\_Blockchain\\_BCI\\_20211117.pdf](https://www.bc-init.at/files/Gutachten_Dokumenten-Notarisierung_Blockchain_BCI_20211117.pdf)

Dokumenten-Notarisierung  
auf Basis Blockchain



erstellt von

**Mag. Dipl.-Ing. Dr. Markus Knasmüller**  
Allgemein beideter und gerichtlich zertifizierter Sachverständig

im Auftrag von

**Blockchain Initiative Austria**  
Anton-Krieger-Gasse 83  
A – 1230 Wien

### Zusammenfassende Bewertung

In dieser privatgutachterlichen Stellungnahme wurde die „Dokumenten-Notarisierung“ auf Basis Blockchain, wie sie vom Verein „Blockchain Initiative Austria“ angeboten wird, untersucht.

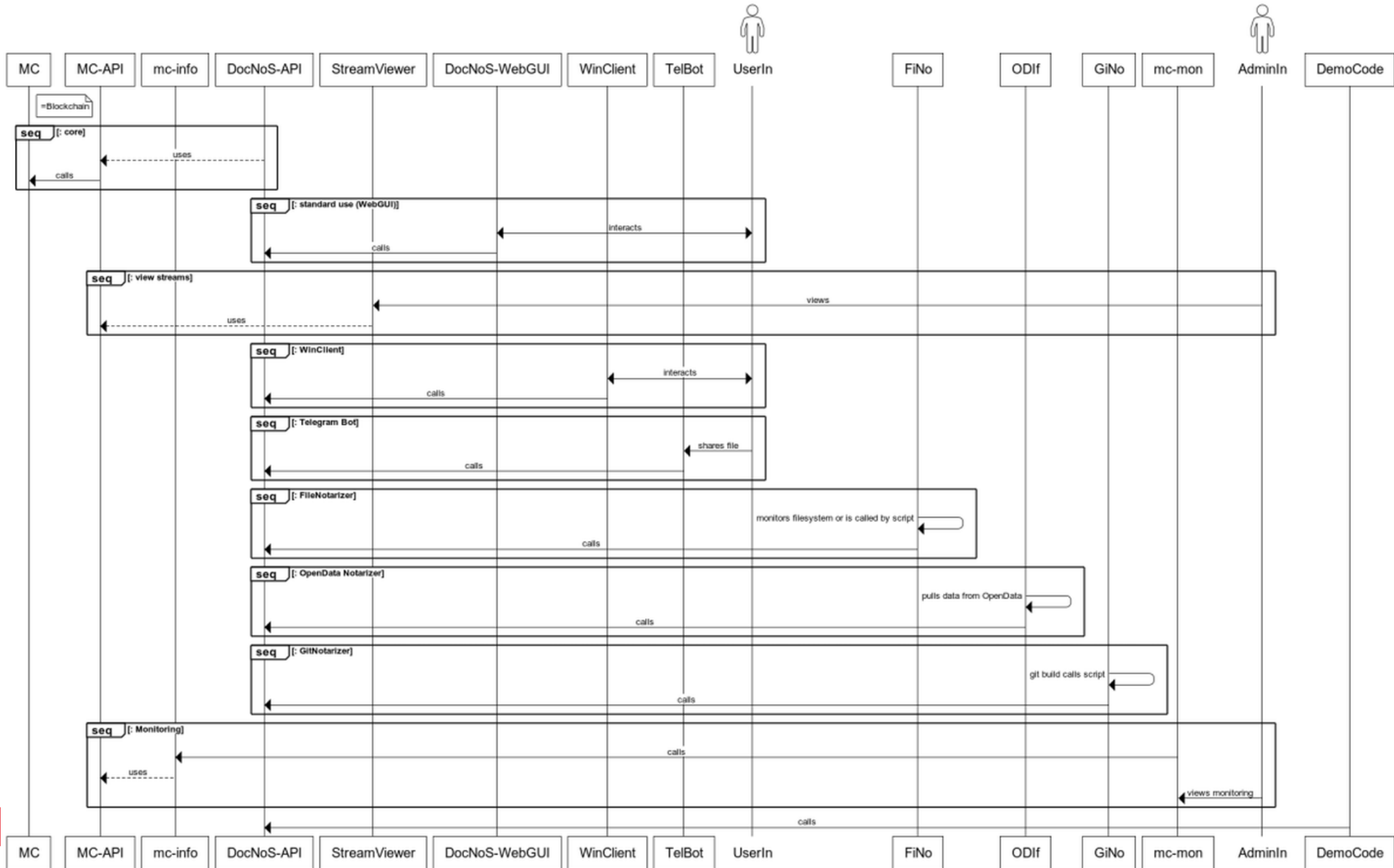
Zusammenfassend lässt sich folgendes festhalten:

- Die verwendete Hashmethode SHA-256 gilt laut der BSI-TR 02102 als kryptographisch stark
- Die zugrundeliegende Blockchain-Bibliothek „MultiChain“ ist eine weit verbreitete Open-Source Plattform, die in vielen Quellen empfohlen wird.
- Das Service ist einfach für jedermann handzuhaben.

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.** Nach Ansicht des unterzeichnenden Sachverständigen entspricht dies jedenfalls dem Stand der Technik und kann zum jetzigen Zeitpunkt nicht widerlegt werden.

Festzuhalten ist allerdings, dass der erbrachte Beweis von der Vertrauenswürdigkeit der Konsortiumsteilnehmer abhängt. Im konkreten Falle ist diese wohl aber mit an Sicherheit grenzender Wahrscheinlichkeit gegeben. Als zusätzliche Sicherheitsstufe ist auch eine Einsicht in die Blockchain möglich.

### DocNoS Landscape & Artifacts




# PSBC - How to participate?

- Try it out (using DocNoS-API on a test chain)
  - get demo code from Github  
<https://github.com/austriapro/blockchain/tree/master/docnos3-testclient>
  - request API-Key - [hello@bc-init.at](mailto:hello@bc-init.at)
  - run it ...
- Implement some application ...
- Productive system
  - become a member of bc-init.at
  - run the application on prod. System
  - ...
  - run a node

# Verification using „Dual Verify“

- Cross-system search
  - APSB: WKO, Wien, WU, BMSGPK ...
  - PSBC: proof.li, docnodes, K&P ...
- Improving usability
- Closer coupling of systems

Blockchain-Service Datenzertifizierung

## Überprüfen einer Datenzertifizierung

Sie können hier überprüfen ob/wann ein Dokument zertifiziert (notarisiert) hinterlegt wurde.  
Wählen Sie dazu das entsprechende File aus (der Hashwert wird automatisch).

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

Zu verifizierende Datei auswählen, um den Hashwert im Browser zu hochgeladen.

Keine Datei ausgewählt.

Digitaler Fingerabdruck (Hashwert sha256)

Alternativ Transaktions-ID eingeben:

Optional: Alle Details anzeigen

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

### 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	006f93cfd535bd35d1f0fd3b808d7a85fc0c09df18d7a83146bb626f261ee9
Bestätigungen	21616

# APSB & PSBC

- Commonalities
  - Principles
  - Technology
  - Usecase data certification
  - Legal Report (available for both systems)
- Differences
  - Legally
    - APSB: own participation rules (see APSB agreement - eGovernment recommendation)
    - PSBC: freer rules, more flexible (association member)
  - Minimal technical differences (data structure, APIs, VPN)

# Summary

- Blockchain initiatives in AT
  - Public area
  - private area
- Operational since around 2019/2020
- Technically structured as “consortium chains”.
  - Authentication for writing, public reading
  - NO proof of work - no energy “waste”
- Currently used for data certification (notarization)
- Further applications in preparation

# The end ...

- Questions?