
„Proof of Existence“

**Unmanipulierbare Protokollierung und unveränderbare
Speicherung von dezentral gemeldeten (Gesundheits-) Daten
mit Hilfe der Blockchain-Technologie**

**DI Dr. Christian Baumann
BMSGPK**

ADV e-Government Konferenz - 28.9.2021

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

Zu meiner Person ...

- TU Wien (Maschinenbau, Informatik)
- Seit > 30 Jahren selbständig im Bereich IT-Consulting
- Projekte u.a. in
 - e-Government, e-Zustellung, digitale Signatur, Bürgerkarte ...
 - BMG: u.a. Aufbau EMS (Epidemiologisches Meldesystem & Outbreak Modul), Heimtierdatenbank ...
 - Diverse Projekte zum Einsatz von Blockchain Technologien (seit 2014) zur „Daten-Zertifizierung“, in öffentlichen und privaten Systemen.
 - Aktuell BMSGPK: technische Themen zu eHN (DCC) und OpenNCP

Statement

Die Blockchain Technologie ermöglicht eine eindeutige, nicht manipulierbare Protokollierung von Datenflüssen und eine unveränderbare Speicherung der Daten mit vollständiger Historisierung. Das ist die Basis für Transparenz und Vertrauenswürdigkeit.

Disclaimer: Inhalte sind meine Meinung und nicht die offizielle Meinung des Gesundheitsministeriums (BMSGPK)

Inhalt

- Problemstellung
- Lösungsansatz?
- Blockchains
 - Eigenschaften
 - Kryptografie
- Lösungsansatz!
- Proof Of Existence / Notarization
 - Austrian Public Service Blockchain
 - 3 Systeme im Echtbetrieb
 - Weitere Beispiele

Disclaimer: Abbildungen Wikipedia (CC0 1.0 oder gemeinfrei)

Problemstellung

- Daten entstehen an dezentralen Stellen ...
- ... müssen in ein System „eingetragen“ werden (manuell, automatisiert)
- Gesammelter Datenbestand -> Auswertungen, z.B.
 - öffentlich abrufbare Dashboards, Export nach Open Data ...
- Teile der Daten falsch? Fällt auf das Gesamtsystem zurück ...
- Korrekturen passieren oft „auf Zuruf“
 - z.B. Daten werden direkt in der DB editiert
- Es ist nicht nachvollziehbar, wer wann welche Daten gemeldet, nachgemeldet, korrigiert hat
- Datenqualität?
- Verantwortung?

Lösungsansatz?

- Einsatz der Blockchain Technologie zur
- dezentralen Erfassung von Daten
 - manuell oder über Interfaces
- exakten nicht manipulierbaren Protokollierung
 - wer hat wann welche Daten geliefert bzw. korrigiert und
- unveränderlichen Speicherung der Daten
 - komplette Historie, auch Korrekturen
- als Basis für nachvollziehbare Auswertungen, Dashboards, OpenData

Blockchains - Eigenschaften

- Dezentral („Peer To Peer“)
 - Blockchain auf alle Teilnehmer verteilt
 - => Alle gleichberechtigt, keine „Zentrale“
 - Datenbank, Netzwerk sehr robust (Ausfallssicherheit)
 - => nicht (bzw. sehr schwer) zerstörbar
- Transparent
 - Alle Teilnehmer haben konsistente Sicht auf alle Daten
 - „Eine Wahrheit“
- Unveränderbar
 - Neue Daten nur hinzufügen
 - Bestehende Daten unveränderbar/unlöschar
- Vertrauen durch Kryptografie
 - Digitaler Fingerabdruck (Hashfunktionen)
 - Digitale Signatur & Verschlüsselung

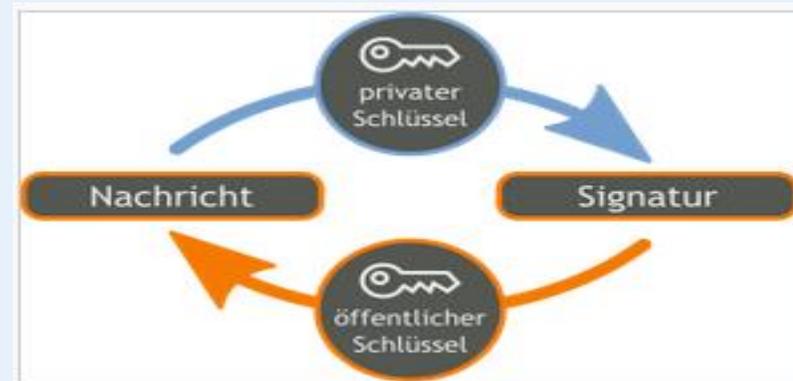
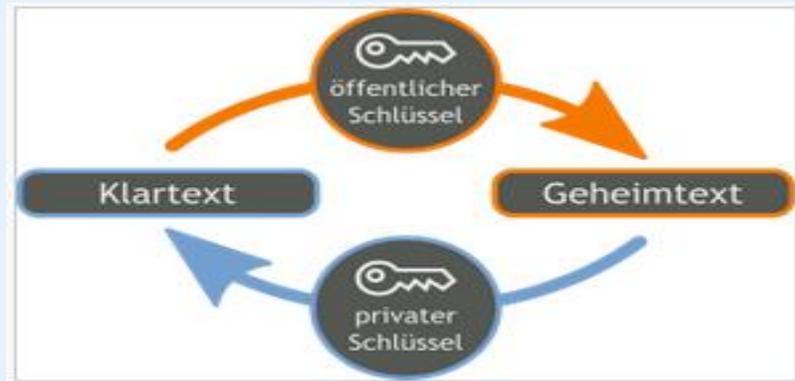
Kryptografie 1/2

- Kryptografischen Hashfunktionen
 - Digitaler Fingerabdruck von Daten
 - Geringste Änderungen Input => große Änderungen Output
 - Unabhängig von der Länge der Daten
 - Eindeutig reproduzierbar
 - Vom Hashwert kann man nicht zu den Daten „zurückrechnen“

Daten	Hash (sha256)
Kaufpreis EUR 10.000,-	5785f79d6fcff99c1a5ffdbf12518c4c973368e06e3a70cfb87477b32bf8da92
Kaufpreis EUR 10.001,-	55a19ba087c6c32b0cdbc16a5167cf11275615c11feada4bc5b0effc3a236e8f
X	4b68ab3847feda7d6c62c1fbcbeebfa35eab7351ed5e78f4ddadea5df64b8015
Das ist ein langer Text, der Hashwert ist aber trotzdem nicht länger ...	0ef31bda0f5fc71152001886cb0e8dc3792565b7df471dcc74ef4fc4bb4c970c

Kryptografie 2/2

- „Public Key Kryptografie“
 - Schlüsselpaar: öffentlicher & privater Schlüssel
 - „asymmetrische“ Verfahren
 - Verschlüsselung mit öffentlichem Schlüssel des Empfängers
 - Empfänger entschlüsselt mit privatem Schlüssel
 - Digitale Signatur mit eigenem privatem Schlüssel
 - Prüfung mit öffentlichem Schlüssel



Lösungsansatz!

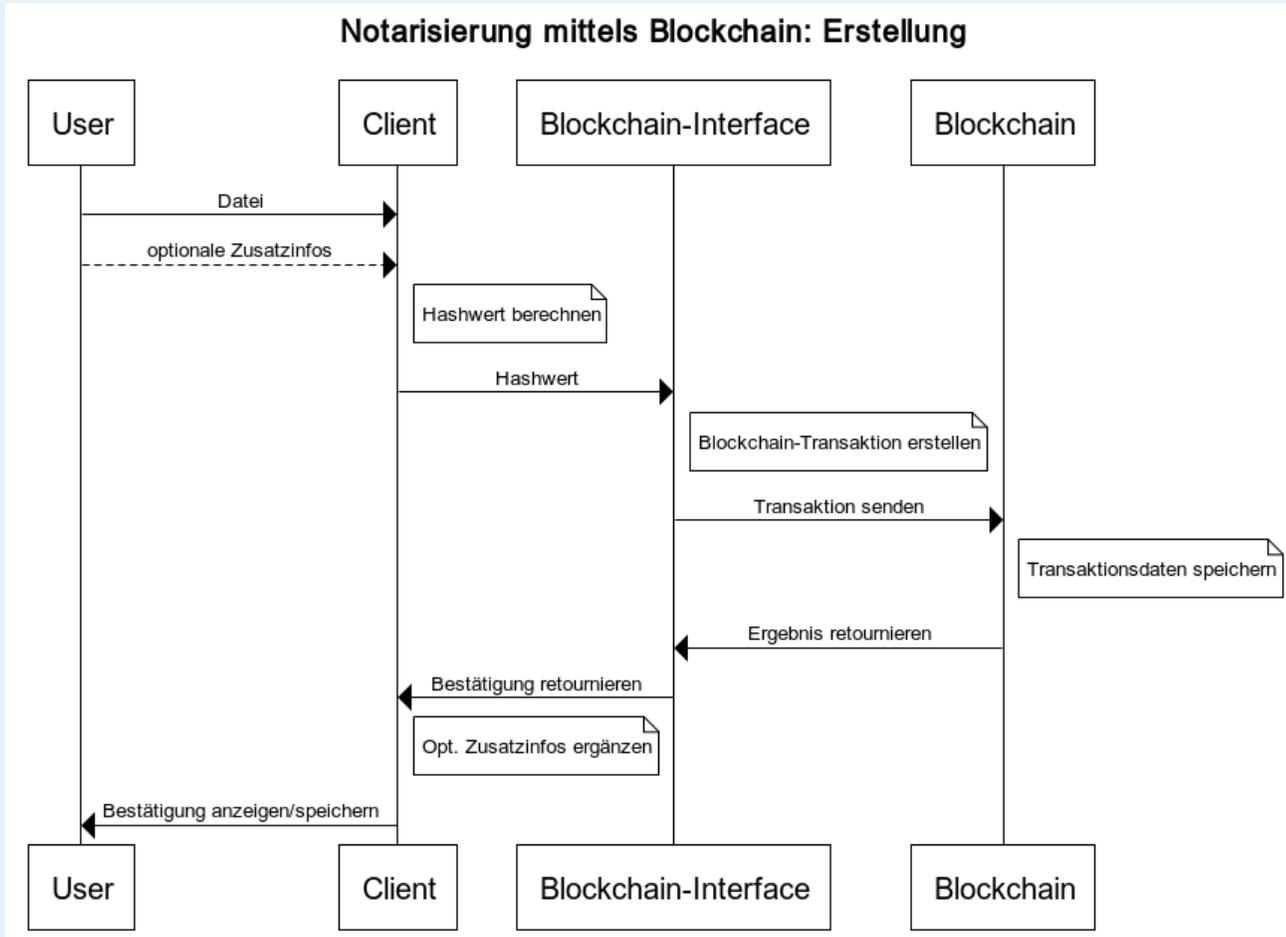
- dezentrale Erfassung von Daten
 - manuell oder über Interfaces
 - Mehrere (alle relevanten) Teilnehmer betreiben Blockchain Nodes
 - Interfaces über aktuelle Protokolle (REST: https/Json)
- exakte nicht manipulierbare Protokollierung
 - wer hat wann welche Daten geliefert bzw. korrigiert und
 - Wer: Alle Teilnehmer (Systeme) sind mit public/private Keys ausgestattet
 - Alle Daten (Transaktionen) werden digital signiert
 - Wann: Zeitstempel der Blöcke eindeutig
- unveränderliche Speicherung der Daten
 - komplette Historie, auch Korrekturen
 - Unlösbarkeit von Daten
 - Absicherung durch Hashfunktionen
- als Basis für nachvollziehbare Auswertungen, Dashboards, OpenData
 - Interfaces über aktuelle Protokolle (REST: https/Json)

„Proof Of Existence“ - „Notarization“

- Mit Notarisierung kann bewiesen werden, dass ein
 - elektronisches Dokument(*)
 - zu einem bestimmten Zeitpunkt
 - in einer bestimmten Form existiert hat und
 - seither nicht verändert wurde.
- Die Sicherheit und das Vertrauen,
 - dass hinterlegte Daten nicht manipuliert werden können, werden dabei durch die Blockchain-Technologie gewährleistet.
- Es werden ausschließlich anonyme Daten verarbeitet!
 - Hashwerte von elektronischen Dokumenten
 - Jedenfalls KEINE personenbezogenen (oder Gesundheits-) Daten

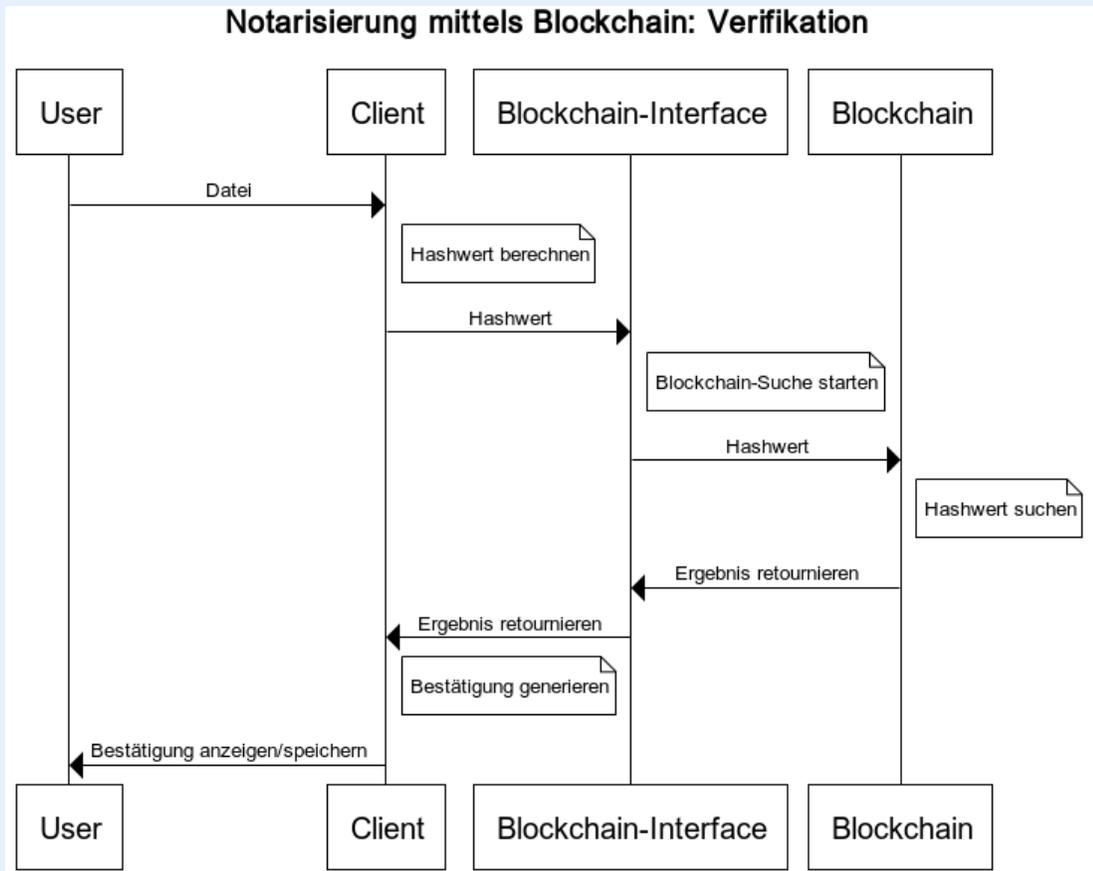
„Dokumente“ = Alle Arten von Daten bzw. Files: Texte, Grafiken, Fotos, Audio, Video, Datenbanken, Logfiles ...

Ablauf - Erstellung



- Hashwert wird am Client errechnet
- D.h. Datei bleibt in Usersphäre
- Ev. Zusatzinfos (Dateiname, Anmerkungen ...) werden NICHT in der Blockchain gespeichert

Ablauf - Verifikation



Mögliche Ergebnisse

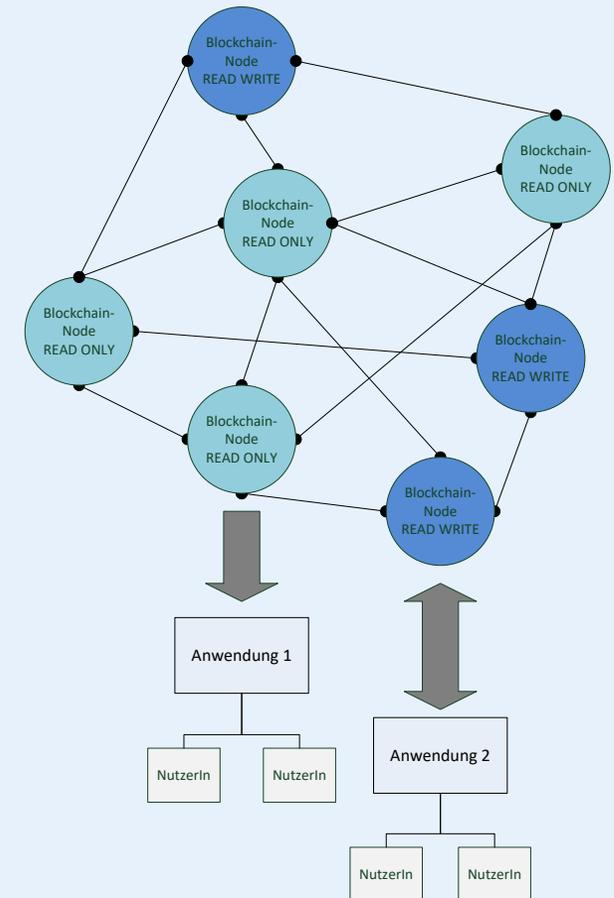
- KEIN Match: „Dieses Dokument wurde nicht in diesem System notarisiert“
- EIN Match: „Dieses Dokument wurde zum [Zeitstempel] notarisiert.“
- MEHRERE Matches: „Ältester Eintrag ist der relevante.“

Erweiterung der Notarisierung

- Notarisierung (von Dokumenten/Files)
 - Ablegen von Hashwerten
 - Betroffene Daten bleiben „off-chain“
- Notarisierung von Daten
 - Ablegen der betroffenen Daten selbst – „on-chain“
 - Varianten
 - End-to-end verschlüsselt (für 2 oder mehrere Teilnehmer)
 - Unverschlüsselt: für Daten, die sowieso publiziert werden

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: Notarisierung
 - Stadt Wien: OGD Notarisierung
 - BRZ (Bundesrechenzentrum)
 - Nic.at (cert.at)
- Angefragt
 - Kontrollbank, FH St. Pölten, TU Wien ...



Austrian Public Service Blockchain (APSB) Vereinbarung

- Inhalt
 - Gegenstand und Zweck
 - APSB-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 zur APSB
 - Technische Spezifikation
 - Kooperationsvereinbarung zur gemeinsamen Weiterentwicklung

Ziel 12/2021: Finales Version
am e-Government Reference
Server



Austrian Public Service Blockchain (APSB) Vereinbarung		ergänzend
		ansb 0.9
		Empfehlung
Kurzbeschreibung:	<p>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.</p> <p>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.</p> <p>Die dabei verwendeten Konsensalgorithmen stellen sicher, dass kein energieverschwendendes Mining betrieben wird und die Infrastruktur auch umwelt- und ressourcenschonend gestaltet ist.</p> <p>In dieser Vereinbarung sind Rechte und Pflichten der APSB-Teilnehmer sowie Standards und Empfehlungen zur Nutzung der APSB enthalten.</p>	

„Daten-Zertifizierung“

- Von WKO geprägter, alternativer Begriff für „Notarisierung“
- Ein digitales Service für
 - WKO Mitglieder
 - und interne Verwendung
- Echtbetrieb seit 11/2019
 - Im Rahmen der „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

- <https://mein.wko.at>

WKO  Mein WKO

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**

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 Blockchain	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

„Unabhängiges“ Verifikationsservice

- Verifikation der Daten von mehreren (allen zukünftigen) Services
- <https://daten-zertifizierung.at/verify/>

Überprüfen einer Datenzertifizierung

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

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

Dokument auswählen
 Keine Datei ausgewählt.

Digitaler Fingerabdruck (Hashwert sha256)

oder Transaktions-ID

Ergebnis der Verifikation

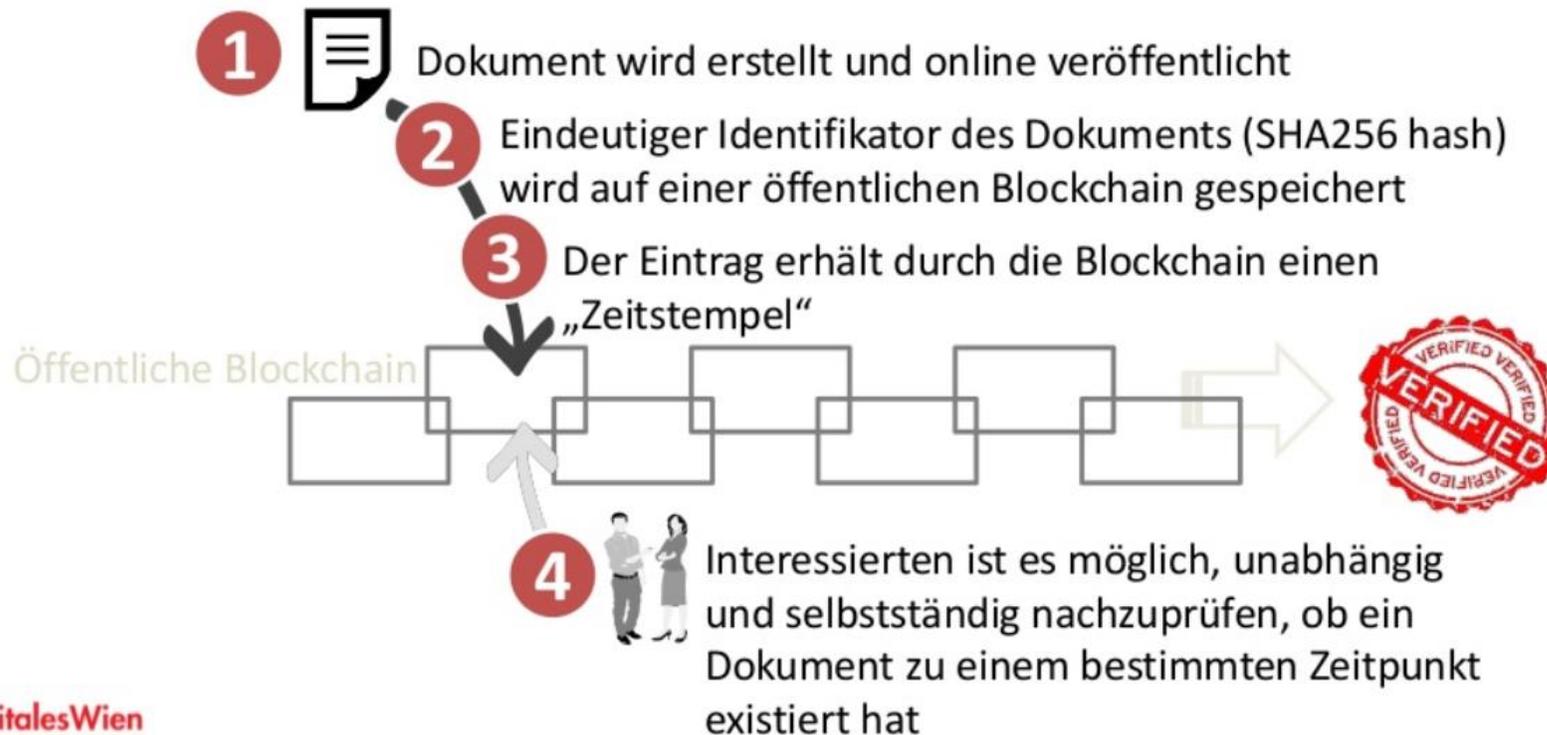
 Hashwert "2a1bea43d639b437dbf05ad72189238a5101246f18651fdc41e37d90b81eb592" gefunden.

Eintrag 1/1

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

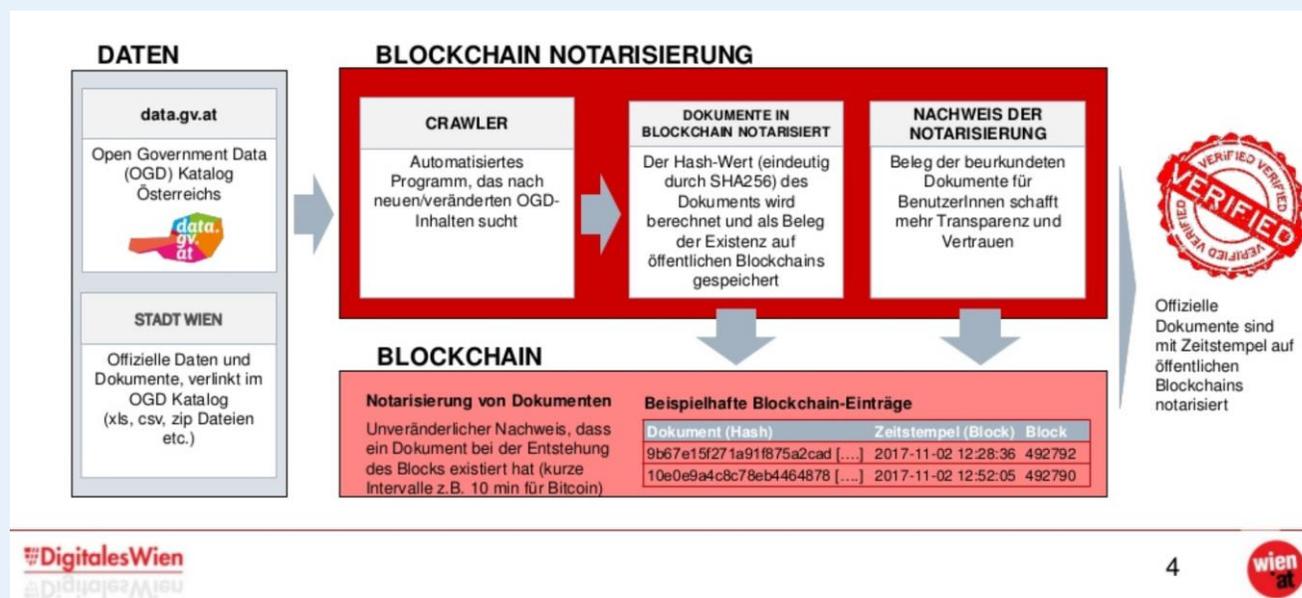
„Notarisierung in Wien“

Die Blockchain ermöglicht nachvollziehbare, öffentliche Nachweise ohne zentrale Autorität



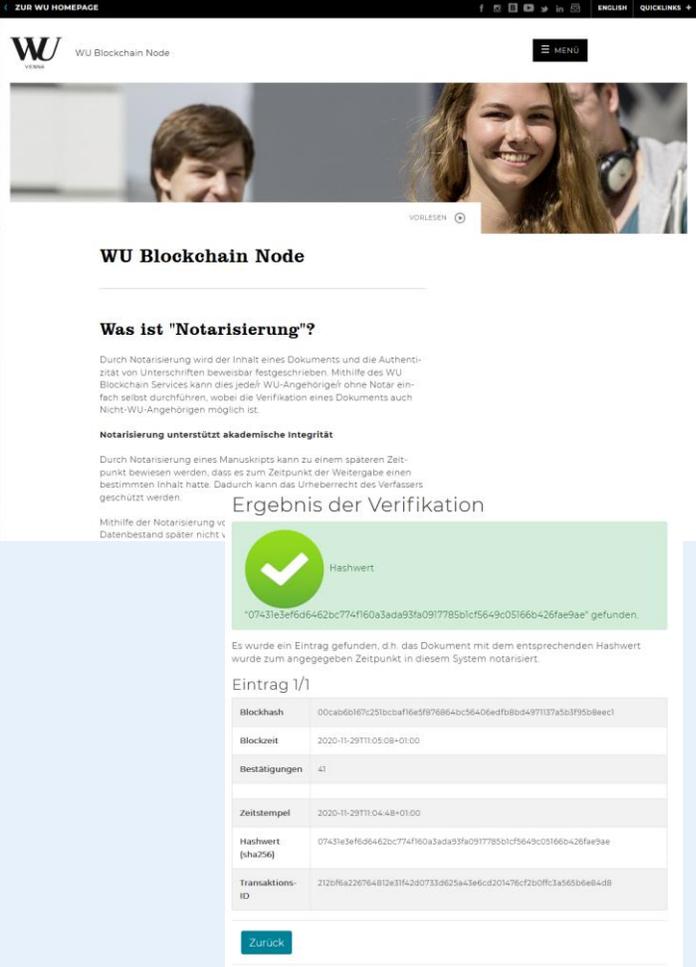
Absicherung der Integrität von Open Government Data durch Hashwerte in einer Blockchain

- Dez. 2017: 1. Blockchain-Pilot
- Aktuelles Projekt: Umbau der Blockchain Infrastruktur auf APSB



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

- Echtbetrieb seit 12/2020
- Use-Case Notarisierung – **Akademische Integrität**
 - Manuskripte – Urheberrecht des Verfassers
 - Daten – Datenbestand nicht verändert (kein Anpassen von empirischen Erhebungen an Hypothesen)
 - Zeugnisse, Bestätigungen und Zertifikate (tlw. in Kombination mit Amtssignatur)



The screenshot shows the 'WU Blockchain Node' website. The main heading is 'WU Blockchain Node'. Below it, there is a section titled 'Was ist "Notarisierung"?' which explains that notarization proves the content of a document and the authenticity of the signature. It also states that 'Notarisierung unterstützt akademische Integrität' (Notarization supports academic integrity) by proving the time of a document's submission. A green box displays the 'Ergebnis der Verifikation' (Verification Result) with a green checkmark and the text: 'Hashwert "07431e3ef6d6462bc774f160a3ada93fa0917785b0cf5649c051660426fae9ae" gefunden.' Below this, a table shows the verification details for 'Eintrag 1/1':

Blockhash	00cab6b07c251bccaf16e5f976864bc56406edfb8bd4971137a5b3f95b08eect
Blockzeit	2020-11-29T11:05:08+01:00
Bestätigungen	41
Zeitstempel	2020-11-29T11:04:48+01:00
Hashwert (sha256)	07431e3ef6d6462bc774f160a3ada93fa0917785b0cf5649c051660426fae9ae
Transaktions-ID	212b6a22676a812e3142d07338625a43e6cd201476cf2b0ffc3a565b6e84d8

A blue button labeled 'Zurück' is visible at the bottom of the page.

Weitere Beispiele

- Meßdaten – Air Quality Chain
- Grundbuch

Protokollierung von (Meß-)daten

- Protokollierung, unveränderliche dezentrale Speicherung und Verteilung
- Beispiel: „Air Quality Chain“ - Umweltmessdaten
- Warum Blockchain?
 - Sichere Speicherung
 - (nachträglich) unveränderbar
 - Dezentral
 - Keinen zentralen Verantwortlichen (u.a. mehrere Admins)
 - Redundanz (ausfallssicher), System nicht „abschaltbar“
 - Vorteile bei Integration
 - Viele, verteilte Daten-Lieferanten
 - Unterschiedliche Schnittstellen & Datenformate
- => Livesystem siehe <https://datnos.com/aqc/>



Protokollierung von offiziellen (Meß-)daten von ...

Stream: aqc-messdaten – 1000 of 7530 items with key: KEND

Publishers	MC2.0a@FRA (1AW7CVnQwpkPvxM7Hun3EYzfZKDZPFNDpHSE3)
Key	KEND
Data	{ "station": "KEND", "zeit": "2018-09-03T11:00:00+02:00", "werte": { "WG": 1.73, "L": 1.0, "NO2": 1.0, "O3": 1.0, "PM10": 1.0, "PM25": 1.0, "SO2": 1.0, "CO": 1.0, "NO": 1.0, "NH3": 1.0, "H2S": 1.0, "H2": 1.0, "CH4": 1.0, "C2H6": 1.0, "C3H8": 1.0, "C4H10": 1.0, "C5H12": 1.0, "C6H14": 1.0, "C7H16": 1.0, "C8H18": 1.0, "C9H20": 1.0, "C10H22": 1.0, "C11H24": 1.0, "C12H26": 1.0, "C13H28": 1.0, "C14H30": 1.0, "C15H32": 1.0, "C16H34": 1.0, "C17H36": 1.0, "C18H38": 1.0, "C19H40": 1.0, "C20H42": 1.0, "C21H44": 1.0, "C22H46": 1.0, "C23H48": 1.0, "C24H50": 1.0, "C25H52": 1.0, "C26H54": 1.0, "C27H56": 1.0, "C28H58": 1.0, "C29H60": 1.0, "C30H62": 1.0, "C31H64": 1.0, "C32H66": 1.0, "C33H68": 1.0, "C34H70": 1.0, "C35H72": 1.0, "C36H74": 1.0, "C37H76": 1.0, "C38H78": 1.0, "C39H80": 1.0, "C40H82": 1.0, "C41H84": 1.0, "C42H86": 1.0, "C43H88": 1.0, "C44H90": 1.0, "C45H92": 1.0, "C46H94": 1.0, "C47H96": 1.0, "C48H98": 1.0, "C49H100": 1.0, "C50H102": 1.0, "C51H104": 1.0, "C52H106": 1.0, "C53H108": 1.0, "C54H110": 1.0, "C55H112": 1.0, "C56H114": 1.0, "C57H116": 1.0, "C58H118": 1.0, "C59H120": 1.0, "C60H122": 1.0, "C61H124": 1.0, "C62H126": 1.0, "C63H128": 1.0, "C64H130": 1.0, "C65H132": 1.0, "C66H134": 1.0, "C67H136": 1.0, "C68H138": 1.0, "C69H140": 1.0, "C70H142": 1.0, "C71H144": 1.0, "C72H146": 1.0, "C73H148": 1.0, "C74H150": 1.0, "C75H152": 1.0, "C76H154": 1.0, "C77H156": 1.0, "C78H158": 1.0, "C79H160": 1.0, "C80H162": 1.0, "C81H164": 1.0, "C82H166": 1.0, "C83H168": 1.0, "C84H170": 1.0, "C85H172": 1.0, "C86H174": 1.0, "C87H176": 1.0, "C88H178": 1.0, "C89H180": 1.0, "C90H182": 1.0, "C91H184": 1.0, "C92H186": 1.0, "C93H188": 1.0, "C94H190": 1.0, "C95H192": 1.0, "C96H194": 1.0, "C97H196": 1.0, "C98H198": 1.0, "C99H200": 1.0, "C100H202": 1.0, "C101H204": 1.0, "C102H206": 1.0, "C103H208": 1.0, "C104H210": 1.0, "C105H212": 1.0, "C106H214": 1.0, "C107H216": 1.0, "C108H218": 1.0, "C109H220": 1.0, "C110H222": 1.0, "C111H224": 1.0, "C112H226": 1.0, "C113H228": 1.0, "C114H230": 1.0, "C115H232": 1.0, "C116H234": 1.0, "C117H236": 1.0, "C118H238": 1.0, "C119H240": 1.0, "C120H242": 1.0, "C121H244": 1.0, "C122H246": 1.0, "C123H248": 1.0, "C124H250": 1.0, "C125H252": 1.0, "C126H254": 1.0, "C127H256": 1.0, "C128H258": 1.0, "C129H260": 1.0, "C130H262": 1.0, "C131H264": 1.0, "C132H266": 1.0, "C133H268": 1.0, "C134H270": 1.0, "C135H272": 1.0, "C136H274": 1.0, "C137H276": 1.0, "C138H278": 1.0, "C139H280": 1.0, "C140H282": 1.0, "C141H284": 1.0, "C142H286": 1.0, "C143H288": 1.0, "C144H290": 1.0, "C145H292": 1.0, "C146H294": 1.0, "C147H296": 1.0, "C148H298": 1.0, "C149H300": 1.0, "C150H302": 1.0, "C151H304": 1.0, "C152H306": 1.0, "C153H308": 1.0, "C154H310": 1.0, "C155H312": 1.0, "C156H314": 1.0, "C157H316": 1.0, "C158H318": 1.0, "C159H320": 1.0, "C160H322": 1.0, "C161H324": 1.0, "C162H326": 1.0, "C163H328": 1.0, "C164H330": 1.0, "C165H332": 1.0, "C166H334": 1.0, "C167H336": 1.0, "C168H338": 1.0, "C169H340": 1.0, "C170H342": 1.0, "C171H344": 1.0, "C172H346": 1.0, "C173H348": 1.0, "C174H350": 1.0, "C175H352": 1.0, "C176H354": 1.0, "C177H356": 1.0, "C178H358": 1.0, "C179H360": 1.0, "C180H362": 1.0, "C181H364": 1.0, "C182H366": 1.0, "C183H368": 1.0, "C184H370": 1.0, "C185H372": 1.0, "C186H374": 1.0, "C187H376": 1.0, "C188H378": 1.0, "C189H380": 1.0, "C190H382": 1.0, "C191H384": 1.0, "C192H386": 1.0, "C193H388": 1.0, "C194H390": 1.0, "C195H392": 1.0, "C196H394": 1.0, "C197H396": 1.0, "C198H398": 1.0, "C199H400": 1.0, "C200H402": 1.0, "C201H404": 1.0, "C202H406": 1.0, "C203H408": 1.0, "C204H410": 1.0, "C205H412": 1.0, "C206H414": 1.0, "C207H416": 1.0, "C208H418": 1.0, "C209H420": 1.0, "C210H422": 1.0, "C211H424": 1.0, "C212H426": 1.0, "C213H428": 1.0, "C214H430": 1.0, "C215H432": 1.0, "C216H434": 1.0, "C217H436": 1.0, "C218H438": 1.0, "C219H440": 1.0, "C220H442": 1.0, "C221H444": 1.0, "C222H446": 1.0, "C223H448": 1.0, "C224H450": 1.0, "C225H452": 1.0, "C226H454": 1.0, "C227H456": 1.0, "C228H458": 1.0, "C229H460": 1.0, "C230H462": 1.0, "C231H464": 1.0, "C232H466": 1.0, "C233H468": 1.0, "C234H470": 1.0, "C235H472": 1.0, "C236H474": 1.0, "C237H476": 1.0, "C238H478": 1.0, "C239H480": 1.0, "C240H482": 1.0, "C241H484": 1.0, "C242H486": 1.0, "C243H488": 1.0, "C244H490": 1.0, "C245H492": 1.0, "C246H494": 1.0, "C247H496": 1.0, "C248H498": 1.0, "C249H500": 1.0, "C250H502": 1.0, "C251H504": 1.0, "C252H506": 1.0, "C253H508": 1.0, "C254H510": 1.0, "C255H512": 1.0, "C256H514": 1.0, "C257H516": 1.0, "C258H518": 1.0, "C259H520": 1.0, "C260H522": 1.0, "C261H524": 1.0, "C262H526": 1.0, "C263H528": 1.0, "C264H530": 1.0, "C265H532": 1.0, "C266H534": 1.0, "C267H536": 1.0, "C268H538": 1.0, "C269H540": 1.0, "C270H542": 1.0, "C271H544": 1.0, "C272H546": 1.0, "C273H548": 1.0, "C274H550": 1.0, "C275H552": 1.0, "C276H554": 1.0, "C277H556": 1.0, "C278H558": 1.0, "C279H560": 1.0, "C280H562": 1.0, "C281H564": 1.0, "C282H566": 1.0, "C283H568": 1.0, "C284H570": 1.0, "C285H572": 1.0, "C286H574": 1.0, "C287H576": 1.0, "C288H578": 1.0, "C289H580": 1.0, "C290H582": 1.0, "C291H584": 1.0, "C292H586": 1.0, "C293H588": 1.0, "C294H590": 1.0, "C295H592": 1.0, "C296H594": 1.0, "C297H596": 1.0, "C298H598": 1.0, "C299H600": 1.0, "C300H602": 1.0, "C301H604": 1.0, "C302H606": 1.0, "C303H608": 1.0, "C304H610": 1.0, "C305H612": 1.0, "C306H614": 1.0, "C307H616": 1.0, "C308H618": 1.0, "C309H620": 1.0, "C310H622": 1.0, "C311H624": 1.0, "C312H626": 1.0, "C313H628": 1.0, "C314H630": 1.0, "C315H632": 1.0, "C316H634": 1.0, "C317H636": 1.0, "C318H638": 1.0, "C319H640": 1.0, "C320H642": 1.0, "C321H644": 1.0, "C322H646": 1.0, "C323H648": 1.0, "C324H650": 1.0, "C325H652": 1.0, "C326H654": 1.0, "C327H656": 1.0, "C328H658": 1.0, "C329H660": 1.0, "C330H662": 1.0, "C331H664": 1.0, "C332H666": 1.0, "C333H668": 1.0, "C334H670": 1.0, "C335H672": 1.0, "C336H674": 1.0, "C337H676": 1.0, "C338H678": 1.0, "C339H680": 1.0, "C340H682": 1.0, "C341H684": 1.0, "C342H686": 1.0, "C343H688": 1.0, "C344H690": 1.0, "C345H692": 1.0, "C346H694": 1.0, "C347H696": 1.0, "C348H698": 1.0, "C349H700": 1.0, "C350H702": 1.0, "C351H704": 1.0, "C352H706": 1.0, "C353H708": 1.0, "C354H710": 1.0, "C355H712": 1.0, "C356H714": 1.0, "C357H716": 1.0, "C358H718": 1.0, "C359H720": 1.0, "C360H722": 1.0, "C361H724": 1.0, "C362H726": 1.0, "C363H728": 1.0, "C364H730": 1.0, "C365H732": 1.0, "C366H734": 1.0, "C367H736": 1.0, "C368H738": 1.0, "C369H740": 1.0, "C370H742": 1.0, "C371H744": 1.0, "C372H746": 1.0, "C373H748": 1.0, "C374H750": 1.0, "C375H752": 1.0, "C376H754": 1.0, "C377H756": 1.0, "C378H758": 1.0, "C379H760": 1.0, "C380H762": 1.0, "C381H764": 1.0, "C382H766": 1.0, "C383H768": 1.0, "C384H770": 1.0, "C385H772": 1.0, "C386H774": 1.0, "C387H776": 1.0, "C388H778": 1.0, "C389H780": 1.0, "C390H782": 1.0, "C391H784": 1.0, "C392H786": 1.0, "C393H788": 1.0, "C394H790": 1.0, "C395H792": 1.0, "C396H794": 1.0, "C397H796": 1.0, "C398H798": 1.0, "C399H800": 1.0, "C400H802": 1.0, "C401H804": 1.0, "C402H806": 1.0, "C403H808": 1.0, "C404H810": 1.0, "C405H812": 1.0, "C406H814": 1.0, "C407H816": 1.0, "C408H818": 1.0, "C409H820": 1.0, "C410H822": 1.0, "C411H824": 1.0, "C412H826": 1.0, "C413H828": 1.0, "C414H830": 1.0, "C415H832": 1.0, "C416H834": 1.0, "C417H836": 1.0, "C418H838": 1.0, "C419H840": 1.0, "C420H842": 1.0, "C421H844": 1.0, "C422H846": 1.0, "C423H848": 1.0, "C424H850": 1.0, "C425H852": 1.0, "C426H854": 1.0, "C427H856": 1.0, "C428H858": 1.0, "C429H860": 1.0, "C430H862": 1.0, "C431H864": 1.0, "C432H866": 1.0, "C433H868": 1.0, "C434H870": 1.0, "C435H872": 1.0, "C436H874": 1.0, "C437H876": 1.0, "C438H878": 1.0, "C439H880": 1.0, "C440H882": 1.0, "C441H884": 1.0, "C442H886": 1.0, "C443H888": 1.0, "C444H890": 1.0, "C445H892": 1.0, "C446H894": 1.0, "C447H896": 1.0, "C448H898": 1.0, "C449H900": 1.0, "C450H902": 1.0, "C451H904": 1.0, "C452H906": 1.0, "C453H908": 1.0, "C454H910": 1.0, "C455H912": 1.0, "C456H914": 1.0, "C457H916": 1.0, "C458H918": 1.0, "C459H920": 1.0, "C460H922": 1.0, "C461H924": 1.0, "C462H926": 1.0, "C463H928": 1.0, "C464H930": 1.0, "C465H932": 1.0, "C466H934": 1.0, "C467H936": 1.0, "C468H938": 1.0, "C469H940": 1.0, "C470H942": 1.0, "C471H944": 1.0, "C472H946": 1.0, "C473H948": 1.0, "C474H950": 1.0, "C475H952": 1.0, "C476H954": 1.0, "C477H956": 1.0, "C478H958": 1.0, "C479H960": 1.0, "C480H962": 1.0, "C481H964": 1.0, "C482H966": 1.0, "C483H968": 1.0, "C484H970": 1.0, "C485H972": 1.0, "C486H974": 1.0, "C487H976": 1.0, "C488H978": 1.0, "C489H980": 1.0, "C490H982": 1.0, "C491H984": 1.0, "C492H986": 1.0, "C493H988": 1.0, "C494H990": 1.0, "C495H992": 1.0, "C496H994": 1.0, "C497H996": 1.0, "C498H998": 1.0, "C499H1000": 1.0, "C500H1002": 1.0, "C501H1004": 1.0, "C502H1006": 1.0, "C503H1008": 1.0, "C504H1010": 1.0, "C505H1012": 1.0, "C506H1014": 1.0, "C507H1016": 1.0, "C508H1018": 1.0, "C509H1020": 1.0, "C510H1022": 1.0, "C511H1024": 1.0, "C512H1026": 1.0, "C513H1028": 1.0, "C514H1030": 1.0, "C515H1032": 1.0, "C516H1034": 1.0, "C517H1036": 1.0, "C518H1038": 1.0, "C519H1040": 1.0, "C520H1042": 1.0, "C521H1044": 1.0, "C522H1046": 1.0, "C523H1048": 1.0, "C524H1050": 1.0, "C525H1052": 1.0, "C526H1054": 1.0, "C527H1056": 1.0, "C528H1058": 1.0, "C529H1060": 1.0, "C530H1062": 1.0, "C531H1064": 1.0, "C532H1066": 1.0, "C533H1068": 1.0, "C534H1070": 1.0, "C535H1072": 1.0, "C536H1074": 1.0, "C537H1076": 1.0, "C538H1078": 1.0, "C539H1080": 1.0, "C540H1082": 1.0, "C541H1084": 1.0, "C542H1086": 1.0, "C543H1088": 1.0, "C544H1090": 1.0, "C545H1092": 1.0, "C546H1094": 1.0, "C547H1096": 1.0, "C548H1098": 1.0, "C549H1100": 1.0, "C550H1102": 1.0, "C551H1104": 1.0, "C552H1106": 1.0, "C553H1108": 1.0, "C554H1110": 1.0, "C555H1112": 1.0, "C556H1114": 1.0, "C557H1116": 1.0, "C558H1118": 1.0, "C559H1120": 1.0, "C560H1122": 1.0, "C561H1124": 1.0, "C562H1126": 1.0, "C563H1128": 1.0, "C564H1130": 1.0, "C565H1132": 1.0, "C566H1134": 1.0, "C567H1136": 1.0, "C568H1138": 1.0, "C569H1140": 1.0, "C570H1142": 1.0, "C571H1144": 1.0, "C572H1146": 1.0, "C573H1148": 1.0, "C574H1150": 1.0, "C575H1152": 1.0, "C576H1154": 1.0, "C577H1156": 1.0, "C578H1158": 1.0, "C579H1160": 1.0, "C580H1162": 1.0, "C581H1164": 1.0, "C582H1166": 1.0, "C583H1168": 1.0, "C584H1170": 1.0, "C585H1172": 1.0, "C586H1174": 1.0, "C587H1176": 1.0, "C588H1178": 1.0, "C589H1180": 1.0, "C590H1182": 1.0, "C591H1184": 1.0, "C592H1186": 1.0, "C593H1188": 1.0, "C594H1190": 1.0, "C595H1192": 1.0, "C596H1194": 1.0, "C597H1196": 1.0, "C598H1198": 1.0, "C599H1200": 1.0, "C600H1202": 1.0, "C601H1204": 1.0, "C602H1206": 1.0, "C603H1208": 1.0, "C604H1210": 1.0, "C605H1212": 1.0, "C606H1214": 1.0, "C607H1216": 1.0, "C608H1218": 1.0, "C609H1220": 1.0, "C610H1222": 1.0, "C611H1224": 1.0, "C612H1226": 1.0, "C613H1228": 1.0, "C614H1230": 1.0, "C615H1232": 1.0, "C616H1234": 1.0, "C617H1236": 1.0, "C618H1238": 1.0, "C619H1240": 1.0, "C620H1242": 1.0, "C621H1244": 1.0, "C622H1246": 1.0, "C623H1248": 1.0, "C624H1250": 1.0, "C625H1252": 1.0, "C626H1254": 1.0, "C627H1256": 1.0, "C628H1258": 1.0, "C629H1260": 1.0, "C630H1262": 1.0, "C631H1264": 1.0, "C632H1266": 1.0, "C633H1268": 1.0, "C634H1270": 1.0, "C635H1272": 1.0, "C636H1274": 1.0, "C637H1276": 1.0, "C638H1278": 1.0, "C639H1280": 1.0, "C640H1282": 1.0, "C641H1284": 1.0, "C642H1286": 1.0, "C643H1288": 1.0, "C644H1290": 1.0, "C645H1292": 1.0, "C646H1294": 1.0, "C647H1296": 1.0, "C648H1298": 1.0, "C649H1300": 1.0, "C650H1302": 1.0, "C651H1304": 1.0, "C652H1306": 1.0, "C653H1308": 1.0, "C654H1310": 1.0, "C655H1312": 1.0, "C656H1314": 1.0, "C657H1316": 1.0, "C658H1318": 1.0, "C659H1320": 1.0, "C660H1322": 1.0, "C661H1324": 1.0, "C662H1326": 1.0, "C663H1328": 1.0, "C664H1330": 1.0, "C665H1332": 1.0, "C666H1334": 1.0, "C667H1336": 1.0, "C668H1338": 1.0, "C669H1340": 1.0, "C670H1342": 1.0, "C671H1344": 1.0, "C672H1346": 1.0, "C673H1348": 1.0, "C674H1350": 1.0, "C675H1352": 1.0, "C676H1354": 1.0, "C677H1356": 1.0, "C678H1358": 1.0, "C679H1360": 1.0, "C680H1362": 1.0, "C681H1364": 1.0, "C682H1366": 1.0, "C683H1368": 1.0, "C684H1370": 1.0, "C685H1372": 1.0, "C686H1374": 1.0, "C687H1376": 1.0, "C688H1378": 1.0, "C689H1380": 1.0, "C690H1382": 1.0, "C691H1384": 1.0, "C692H1386": 1.0, "C693H1388": 1.0, "C694H1390": 1.0, "C695H1392": 1.0, "C696H1394": 1.0, "C697H1396": 1.0, "C698H1398": 1.0, "C699H1400": 1.0, "C700H1402": 1.0, "C701H1404": 1.0, "C702H1406": 1.0, "C703H1408": 1.0, "C704H1410": 1.0, "C705H1412": 1.0, "C706H1414": 1.0, "C707H1416": 1.0, "C708H1418": 1.0, "C709H1420": 1.0, "C710H1422": 1.0, "C711H1424": 1.0, "C712H1426": 1.0, "C713H1428": 1.0, "C714H1430": 1.0, "C715H1432": 1.0, "C716H1434": 1.0, "C717H1436": 1.0, "C718H1438": 1.0, "C719H1440": 1.0, "C720H1442": 1.0, "C721H1444": 1.0, "C722H1446": 1.0, "C723H1448": 1.0, "C724H1450": 1.0, "C725H1452": 1.0, "C726H1454": 1.0, "C727H1456": 1.0, "C728H1458": 1.0, "C729H1460": 1.0, "C730H1462": 1.0, "C731H1464": 1.0, "C732H1466": 1.0, "C733H1468": 1.0, "C734H1470": 1.0, "C735H1472": 1.0, "C736H1474": 1.0, "C737H1476": 1.0, "C738H1478": 1.0, "C739H1480": 1.0, "C740H1482": 1.0, "C741H1484": 1.0, "C742H1486": 1.0, "C743H1488": 1.0, "C744H1490": 1.0, "C745H1492": 1.0, "C746H1494": 1.0, "C747H1496": 1.0, "C748H1498": 1.0, "C749H1500": 1.0, "C750H1502": 1.0, "C751H1504": 1.0, "C752H1506": 1.0, "C753H1508": 1.0, "C754H1510": 1.0, "C755H1512": 1.0, "C756H1514": 1.0, "C757H1516": 1.0, "C758H1518": 1.0, "C759H1520": 1.0, "C760H1522": 1.0, "C761H1524": 1.0, "C762H1526": 1.0, "C763H1528": 1.0, "C764H1530": 1.0, "C765H1532": 1.0, "C766H1534": 1.0, "C767H1536": 1.0, "C768H1538": 1.0, "C769H1540": 1.0, "C770H1542": 1.0, "C771H1544": 1.0, "C772H1546": 1.0, "C773H1548": 1.0, "C774H1550": 1.0, "C775H1552": 1.0, "C776H1554": 1.0, "C777H1556": 1.0, "C778H1558": 1.0, "C779H1560": 1.0, "C780H1562": 1.0, "C781H1564": 1.0, "C782H1566": 1.0, "C783H1568": 1.0, "C784H1570": 1.0, "C785H1572": 1.0, "C786H1574": 1.0, "C787H1576": 1.0, "C788H1578": 1.0, "C789H1580": 1.0, "C790H1582": 1.0, "C791H1584": 1.0

Anwendungsbeispiel Grundbuch

- Hernando de Soto: *„... nur ein Drittel aller Menschen können beweisen, dass ihnen ihr Land gehört. Abgesehen von der rechtlichen Unsicherheit gibt es dadurch 20 Billionen US-Dollar an totem Kapital, da Land mit ungeklärten Rechtstiteln nicht verkauft werden kann.“*
- Beispiel Ghana: 90% der Grundstücke nicht in der „Landkommission“ registriert.
- Grundbuch ähnlich wie Blockchain strukturiert
 - Hauptbuch
 - gelöschte Eintragungen
 - (Stammdaten)
- Aber zentral
 - Anfällig für Korruption, Betrug, Kriminalität ...
 - (natürlich nicht in Österreich ;-)

Anwendungsbeispiel Grundbuch => Blockchain

- => dezentral, unveränderlich, transparent ...
- Bereits umgesetzt in
 - Georgien (2017): „Korruption, Betrug, Misstrauen“
 - Bürger: Einblick, Kontrollinstanz
 - Staatliche Stellen: gegenseitige Kontrolle
 - Schweden (2017):
 - Zukunftsorientierung
 - Kostenersparnis
- Pilotprojekte u.a. in: Slowenien, Indien, Brasilien, Russland, Dubai, Chicago

Use Case Schweden: Grundbuchamt

- Pilotprojekt zur Nutzung der Blockchain-Technologie um Management von Immobilientransaktionen zu verbessern
- Partner: Lantmäteriet, Telia, ChromaWay, Kairos Future, LHB, SBAB
- Ziel: Blockchain-gestütztes Katasteramt für Schweden
 - Vermeiden von physischen Archiven für Verträge und Dateien
 - Höhere Resilienz und Redundanz von Transaktionsdaten
 - Höhere Sicherheit für Benutzer des Systems
 - Schnellere und transparentere Transaktionen
 - Offizielle Registrierung und Bestätigung von anstehendem Eigentümerwechsel ca. 4 Monate früher als aktuell + sofortige automatische Bestätigung über Grundbucheintrag

Fazit

- Blockchain Technologie
 - Dezentral
 - Transparent
 - Unveränderbar
- Vertrauen durch Kryptografie
 - Kryptografische Hashfunktion, Public Key Kryptographie (Digitale Signatur/Verschlüsselung)
 - Blockchain intern, aber auch auf Anwendungsebene
- In mehreren Bereichen im Echtbetrieb
 - Öffentliche (und privatwirtschaftliche) Anwendungen
 - Erste Anwendungen betreffen „Notarisierung“ (Dokumente und Daten)
 - Austrian Public Service Blockchain (APSB) kann jederzeit neue Mitglieder onboarden!
- Einsatzmöglichkeiten in Ihren Fachbereichen?

Fragen?

DI Dr. Christian Baumann

c.baumann@baumann.at

+43 664 43 24 243