Arbeitskreis Blockchain

Allgemeines &
Arbeitsgruppe Technik & Blockchain Lab

AUSTRIAPRO

Dr. Christian Baumann

22.1.2020

Agenda

- Allgemein
  - Austrian Public Service Blockchain
  - „Datenzertifizierung“ für die Privatwirtschaft
  - Rechtliches Gutachten
- Blockchain-Lab
  - Anchoring
  - Notarisierung vs. Digitale Signatur
  - Weitere Themen
- News
- Openspace

Austrian Public Service Blockchain

- Initiative von Institutionen der öffentlichen Verwaltung
- Aufbau einer „Konsortium-Blockchain“ für unterschiedliche Usecases im „public service“ Bereich
- Beteiligte (Gründung)
  - BRZ (Bundesrechenzentrum)
  - Gemeinde Wien
  - WKO (Wirtschaftskammer)
- Weitere
  - Zugesagt: WU Wien, TU Wien, FH St. Pölten, Kontrollbank
  - Angefragt: nic.at bzw. cert.at, ev. UNO

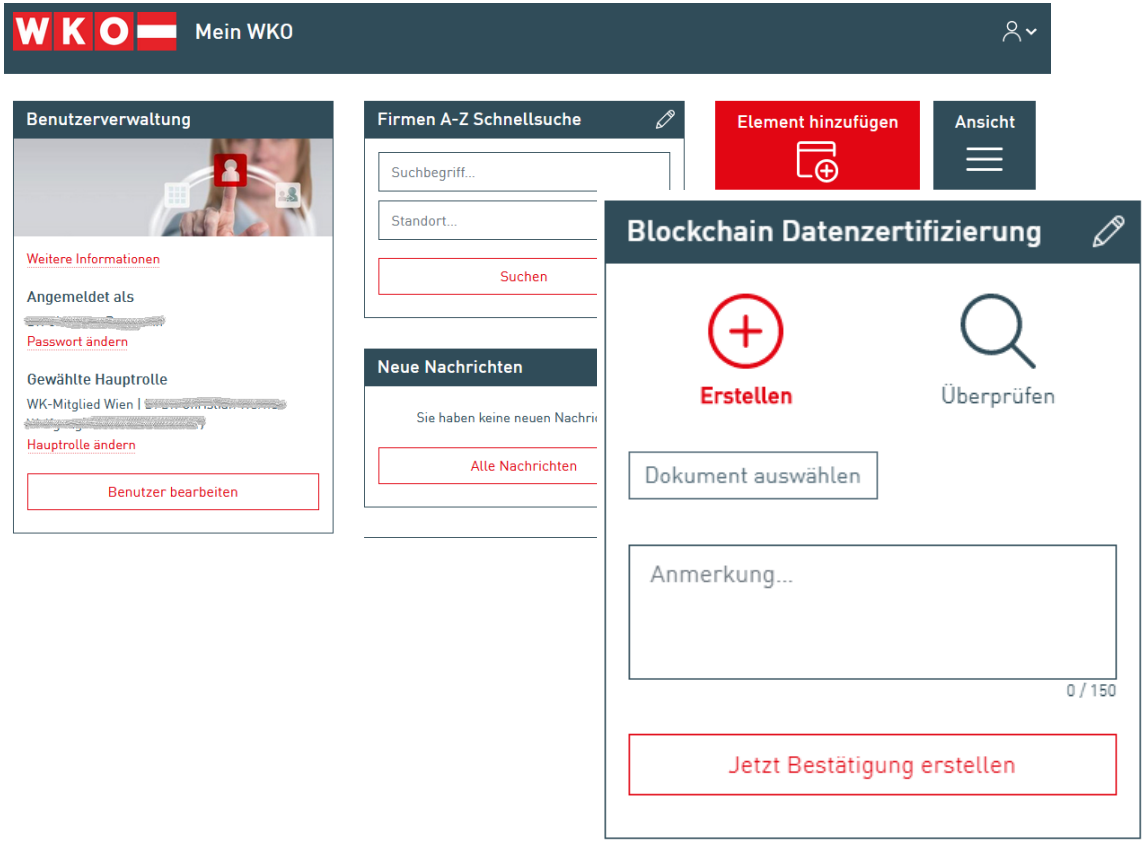
1. Usecase: Notarisierung

- Notarisierung
  - 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
    - (ggf. technische Infos)
    - KEINE personenbezogenen Daten

WKO „Daten-Zertifizierung“

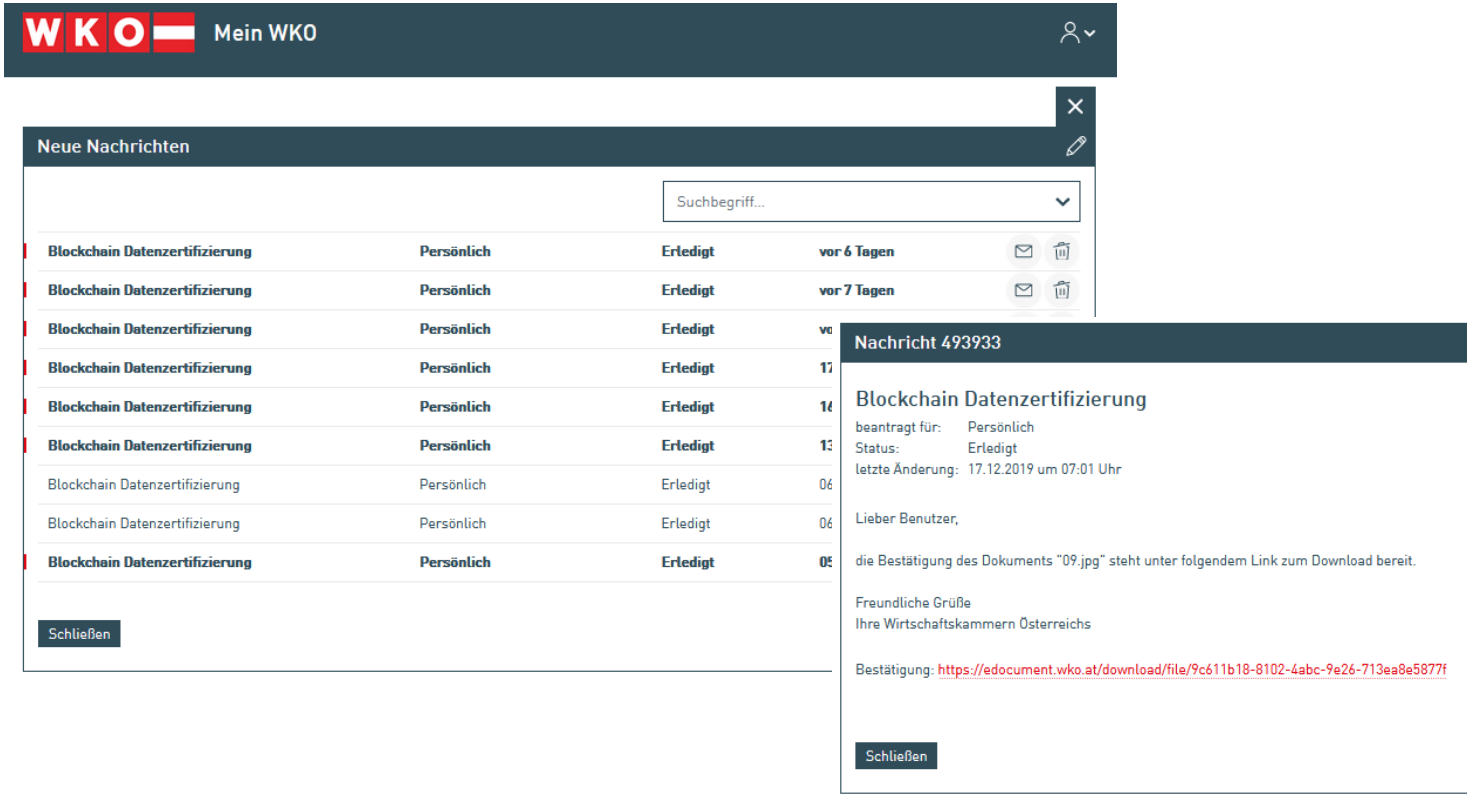
- Anderer Begriff für „Notarisierung“
- Blockchainumgebung siehe „APSBC“
  - Echtbetrieb seit Oktober 2019
- Echtbetrieb GUI unter https://mein.wko.at
  - Seit 6.11.2019: WKO intern, d.h. alle Mitarbeiter
  - Seit 12/2019: Alle User mit WKIS Login
    - Alle WKO Mitglieder
    - Plus weitere registrierte User

GUI im Dashboard „mein.wko.at“



GUI im Dashboard „mein.wko.at“

- Neu: Benachrichtigungen



Status und next steps

- Austrian Public Service Blockchain
  - Vereinbarung zwischen den drei „Gründern“
    - Basierend auf Portalverbundvereinbarung
    - https://www.ref.gv.at/AG-RS-PVV-pvv-1-2-1-15-11.332.0.html
  - Weitere Partner aus öffentl. Verwaltung aufnehmen
  - Weitere Usecases definieren
    - Z.B. Liste der Public Keys von PVP (Idee Wien)
- Daten-Zertifizierung WKO
  - NEU: „Externes“ Verifikationsservice
    - auch für nicht „mein.wko.at“ User
    - und zur Verifikation von Dokumenten anderer Services

„Externes“ Verifikationsservice

- https://datenzertifizierung.at/verify/ oder
- https://daten-zertifizierung.at/verify/

„Datenzertifizierung“ für die Privatwirtschaft

- Bereits mehrere Anfragen aus Privatwirtschaft
- WKO/AP: „Unterstützung einer privaten Konsortialblockchain zur Zertifizierung von Daten”
  - Zielsetzung: Aufbau einer dauerhaften und sicheren Blockchain-Infrastruktur für Österreichs Wirtschaft
  - **Einrichtung und Moderation eines offenen Stakeholder-Forums zum Aufbau und Steuerung der Infrastruktur bzw. Organisation**
  - **Kooperation ABC (WU Wien) und AustriaPro (WKO)**
  - WKO betreibt Blockchain-Knoten (aktuell Testsystem)

„Datenzertifizierung“ für die Privatwirtschaft 1/2

- Systemaufbau
  - Dieselbe technologische Basis wie „Daten-Zertifizierung“
  - Einfachere Regeln wie im öffentlichen Bereich
  - Funktionale Erweiterungen je nach Anforderungen
  - Ausprägung als Konsortiumchain
    - Vertrauenswürdige Unternehmen & Institutionen betreiben die Blockchain Nodes (Schreibzugriff)
    - Öffentlicher Lesezugriff (Read-Only Nodes) zum Validieren der Daten

„Datenzertifizierung“ für die Privatwirtschaft 2/2

- Kosten
  - Kosten für Node
    - Setup & Betrieb
    - Keine Lizenzkosten für Node selbst
  - Keine „Transaktionskosten“
  - Geringe „Verwaltungsgebühr“
    - z.B. Vereinsmitgliedsbeitrag
- Mögliche neue Services für Provider
  - „Blockchain as a Service“ oder
  - „API as a Service“

Status & Next Steps 1/2

- Testsystem
  - Verfügbar (u.a. auch im Blockchain-Lab)
    - Ein paar Unternehmen betreiben bereits Test-Nodes
- Organisation
  - AustriaPro und Austrian Blockchain Center
    - Neu: AustriaPro wurde Partner des ABC
  - Definition Forschungsprojekt
    - Rechtliche und organisatorische Rahmenbedingungen
    - Neu: 1. Entwurf vorliegend

Status & Next Steps 2/2

- Echtsystem
  - Parallel zur „Einrichtung ... des eines offenen Stakeholder-Forums“
    - Dauer der Forschungen noch nicht bekannt
  - Moderation einstweilen durch AustriaPro
  - Start für 2/2020 geplant
  - Erste Anwendungen bereits fixiert

"Daten Zertifizierung" auf Basis Blockchain - Gutachten

- Privatgutachterliche Stellungnahme
  - Dr. Knasmüller (allg. beeideter & ger. zertif. SV)
- APSBC & private Anwendungen
- Geplanter Inhalt
  - Beschreibung System und Funktionsweise
  - Verwendete Technologien & Standards
  - Praktische Versuche
    - im Rahmen des AUSTRIAPRO Blockchain Labs
  - Ggf. Verbesserungsvorschläge

- **Status**: kurz vor Fertigstellung

Blockchain-Lab

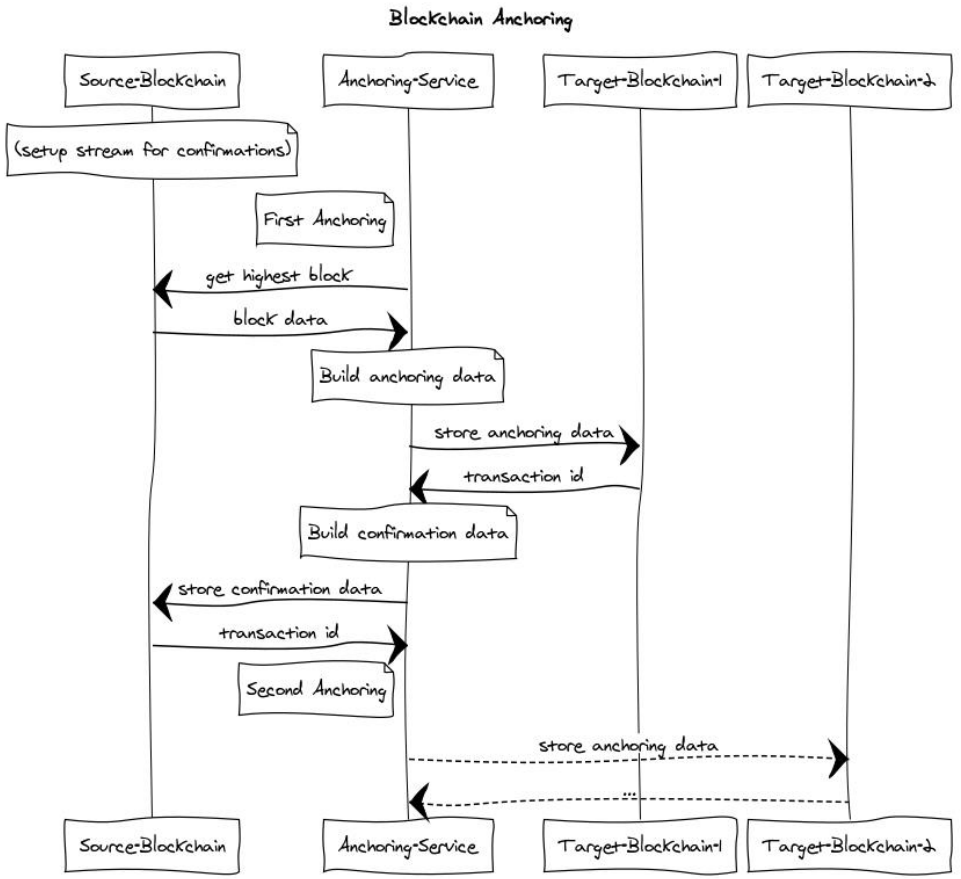
- Anchoring
- Notarisierung vs. Digitale Signatur
- Weitere Themen
  - Self Sovereign Identity (Node Setup ongoing)
  - IoT Identity (Kontakt zu Riddle&Code)
  - ARTIS

Anchoring

- Notarisierung des aktuellen Zustandes einer (z.B. privaten oder Konsortium-) Chain in public Blockchains
- D.h. pot. Manipulationen in einer „kleinen" Chain werden verhindert (bzw. würden erkannt)
- Zustands-Daten
  - Aktueller Block
    - `Blocknummer`
    - `Hash`
    - `Zeitstempel`
  - …

Anchoring - Ablauf

- Anchoring Service bereitet Daten einer Source-Blockchain auf und
- trägt sie in ein oder mehrere Target-Blockchains ein.
- Bestätigung wird in Source-Chain eingetragen



Anchoring

- Beispiele für Target Chains

3. Welche Target Chains?

Target-Blockchain	Anzahl an (Full-) Nodes	Kosten pro Transaktion
Bitcoin	10.000	€ 0,50
Ethereum	12.000	€ 0,10-0,30
...		
Artis	...	...

- Aktueller Status
  - Spezifikation in Ausarbeitung
  - prototypische Implementierung geplant

Notarisierung vs. Digitale Signatur

- Immer wieder gehört: *„Wozu Notarisierung in einer Blockchain, wir haben ja die digitale Signatur?*"

- Technologievergleich zeigt
  - Schließen einander nicht aus
  - Optimale Ergänzung!

- Details %

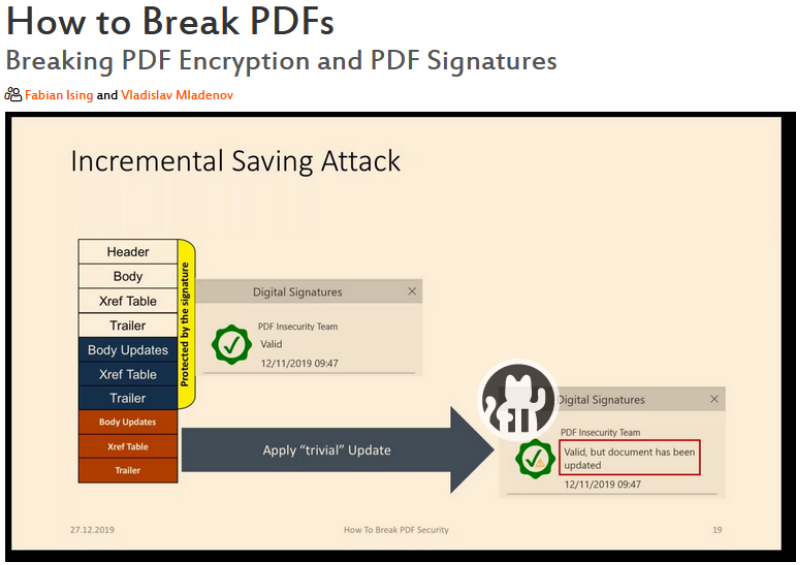
Notarisierung vs. Digitale Signatur

Technologievergleich

	Digitale Signatur	Notarisierung in Blockchain
Public/Private Key Verfahren	Ja	Ja
Zertifikat personenbezogen (Identität)	Ja (Signator)	Nein (Nodebetreiber)
Integrität der Nachricht	Ja	Ja
Zeitstempel garantiert korrekt	Nein	Ja
Fileformate (theoretisch)	Alle	Alle
Fileformate (praktikabel für User!)	PDF	Alle
Signaturumgebung nötig	Chipkarte oder Handysignatur	nein
Erstellung	Online oder Offline	Online
Prüfung	PDF-Reader (Online)	Online (Browser) oder Hashwert mit anderem Tool ermitteln

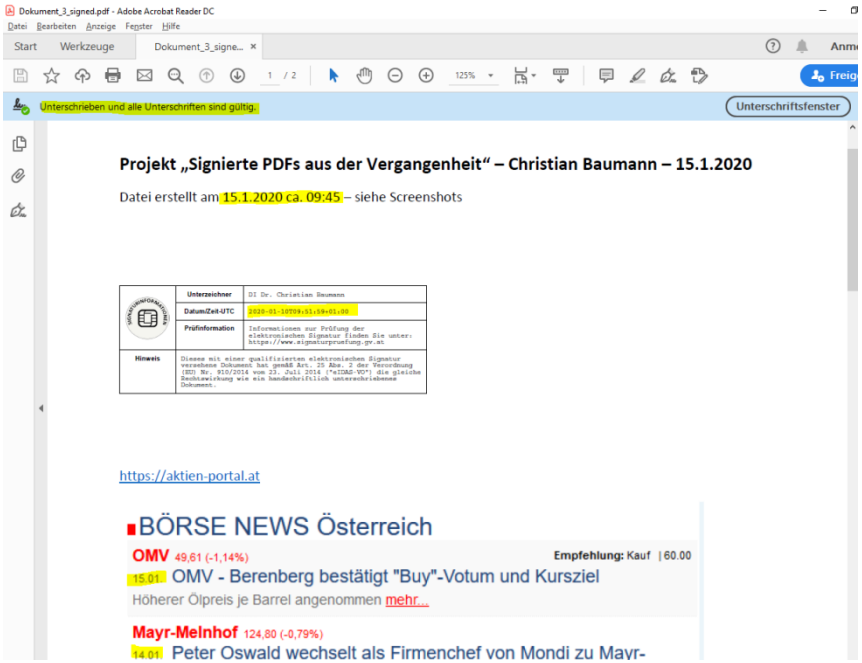
Probleme der PDF Signatur 1/2

- „Breakable“
- https://media.ccc.de/v/36c3-10832-how_to_break_pdfs



Probleme der PDF Signatur 2/2

- Zeitstempel manipulierbar
  - Lokale Signaturumgebung & Handysignatur



Lab - Phase 7: „SSI“

- Self Sovereign Identity
  - Vgl. Network #16
- Neue Module/Systeme im Lab bereitstellen
  - Aktuell: Installation Sovrin „Steward“
    - Z.B. verwendet von https://meinesichereid.org/
    - Konsortium (Banken, Telekom …)
    - Branchenübergreifendes, offenes Trust-Netzwerk …
- **Aktueller Status**
  - Installation Node (etwas verspätet aber ongoing)
- Next Steps
  - Demos & Schnittstellen?

Lab - Phase 7: „IoT-Identity“ 1/2

Blockchain-basierte digitale Identitäten für IoT Devices

- Use-case
  - Blockchain Anwendungen müssen mit der Außenwelt kommunizieren, z.B.
    - z.B. (Sensor-)daten erfassen
    - Aktoren ansteuern
  - Entweder über definierte Nodes oder über „Oracles“
- Problemstellung
  - Daten müssen „vertrauenswürdig“ sein, d.h.
  - 1) Sensoren/Aktoren geprüft, geeicht … nach entsprechenden Normen
  - 2) jeweils eigene eindeutige Identität (unfälschbar, unmanipulierbar)

Lab - Phase 7: „IoT-Identity“ 2/2

- Schwerpunkte im Projekt
  - Demonstration der gesicherten und vertrauenswürdigen Integration solcher Devices in Blockchain Anwendungen
- Hardware
  - (IoT-) Devices mit Kryptofunktionen (Public-Key Kryptografie)
  - Können eigene Identität erzeugen und beweisen
- **Status Umsetzung**
  - Infineon „Blockchain Security 2Go“ – Libraries & Democode vorhanden
  - Riddle & Code – öst. Unternehmen, spezialisiert auf „trusted connections between physical and digital world“

Blockchain Lab – Weitere Themen

- Artis Blockchain
  - lab10 collective (Graz)
  - Focus e-mobility solutions
  - Im Lab: Node im Testnetz
    - http://status.tau1.artis.network/
  - Geplant: Validator-Node im Echtsystem
    - https://artis.eco/
- **Status**
  - Warten auf (stabile) POA-Implementierung

Empfehlungen für (APSBC-) Blockchainknoten

- Bereiche
  - Leistungs-anforderungen
  - Netzwerk
  - Ausfallssicherheit
  - Betriebssystem
  - Weitere Software/Services
- Status: In Ausarbeitung

3.1. Hardware

Physischer oder virtueller Server, die Leistungsanforderungen hängen u.a. vo
Empfehlungen:

	Min. Funktionalität	Max. Funktionalität
Synchronisieren der Blockchain(s) und Speichern der Daten („Read-Only" Node)	X	X
Minimales API (Datenabfrage, Blockexplorer, Monitoring ...)	X	X
Teilnahme am "Konsens" – (Proof Of Authority) d.h. Erstellen von Blöcken	-	X
API für weitere Anwendungen	-	X
CPU	1	2
RAM	2GB	8GB
Disk (SSD empfohlen)	>= 50GB	>= 50GB ++ (je nach Anwendungen)

News 1/2

- Blockchain Award
  - www.blockchainaward.at
  - WKO & Austrian Blockchain Center

News 2/2

- Europäische Kommision „Online questionnaire for European Blockchain Pre-Commercial Procurement is live“

https://ec.europa.eu/newsroom/dae/newsletter-specific-archive-issue.cfm?newsletter_service_id=167&lang=default

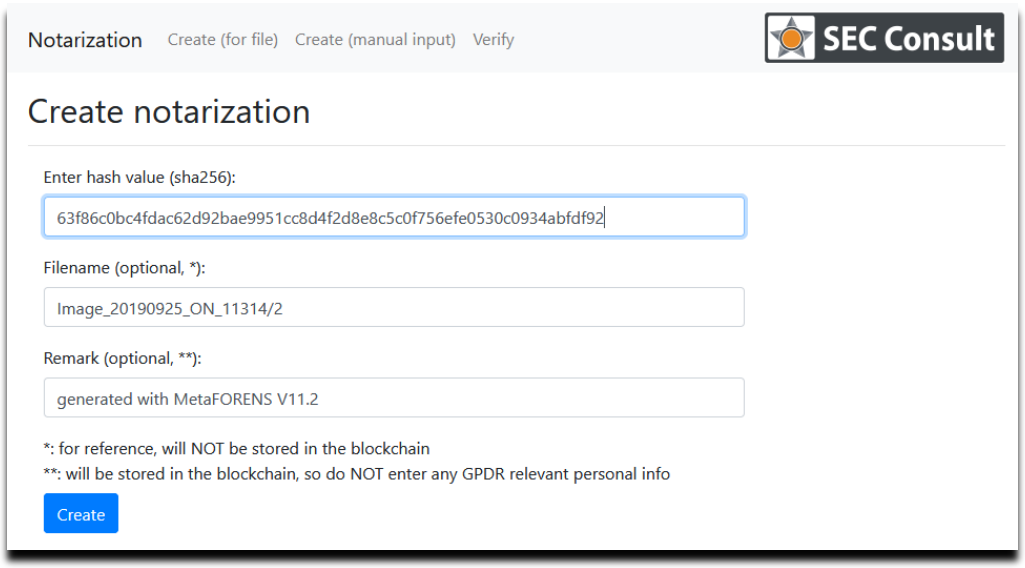
Openspace

- SEC Consult
  - „ForensicForever“
- Digitalisierungsagentur
  - Eduard-Albert Prinz MSc BSc

ForensicForever

- „Blockchain basierte Notarisierung zur Beweissicherung von Daten im Rahmen von forensischen Analysen“
  - Eingabedaten (z.B. Disk-Images) oder
  - anderen Dateien (z.B. erstellte Reports)
- Motivation
  - Maximale Absicherung der betroffenen Daten
  - Z.B. Beweismittel vor Gericht
- Funktionsweise analog Daten-Zertifizierung
  - Erweiterungen der Hash-Generierung
    - Im Browser (kleine Files)
    - Externes Tool (Disk-Images)

Beispiel: Notarisierung mit (manuell) importiertem Hashwert



Blog Beitrag vom 21.1.2020

- Gefördert von TIP-WKNÖ
- Projektergebnis Protptyp

- Erweiterung auf Echtsystem
- „Datenzertifizie-rung für die Privatwirtschaft“

https://sec-consult.com/blog/2020/01/wie-man-die-blockchain-technologie-zur-sicherung-forensischer-beweise-einsetzt/

WIE MAN DIE BLOCKCHAIN-TECHNOLOGIE ZUR SICHERUNG FORENSISCHER BEWEISE EINSETZT

Am 21. Jan 2020

SEC Consult beobachtet seit einiger Zeit die Entwicklung und die Einsatzmöglichkeiten der Blockchain-Technologien. Diese Technologien könnten auch in einzelnen Bereichen des Security-Consultings eingesetzt werden. Im Rahmen eines Forschungsprojekts wurden mögliche Szenarien für die Beweissicherung nach Cyber-Angriffen näher betrachtet.

Warum Blockchain in der Forensik?

Das SEC Consult SEC Defence-Team nutzt zur Analyse von Cyber Incidents diverse Forensik-Tools. Bei immer mehr Analysen stellt sich die Herausforderung, dass die Ergebnisse auch **vor Gericht als Beweismittel** eingesetzt

Openspace

- SEC Consult
  - „ForensicForever“
- Digitalisierungsagentur
  - Eduard-Albert Prinz MSc BSc

Kontakt

AUSTRIAPRO

http://www.austriapro.at
austriapro@wko.at

DI Dr. Christian Baumann
c.baumann@baumann.at
+43 664 43 24 243