Arbeitskreis Blockchain

Allgemeines & Arbeitsgruppe Technik & Blockchain Lab

Dr. Christian Baumann

22.9.2021

AUSTRIA PRO

Agenda

- News zu „Austrian Public Service Blockchain”
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Fragen)
- Vorschau Blockchain Award 2021 (offizielle Verleihung) und eDay 2021
- Kooperation mit DIO (Data Intelligence Offensive)
- open space – spontane Beiträge zu Projekten, Initiativen etc.
  - „Digitaler Frachtbrief & Blockchain“, Alex Schaefer, editel

AUSTRIA PRO

Austrian Public Service Blockchain („APSB“) - Status 9/2021

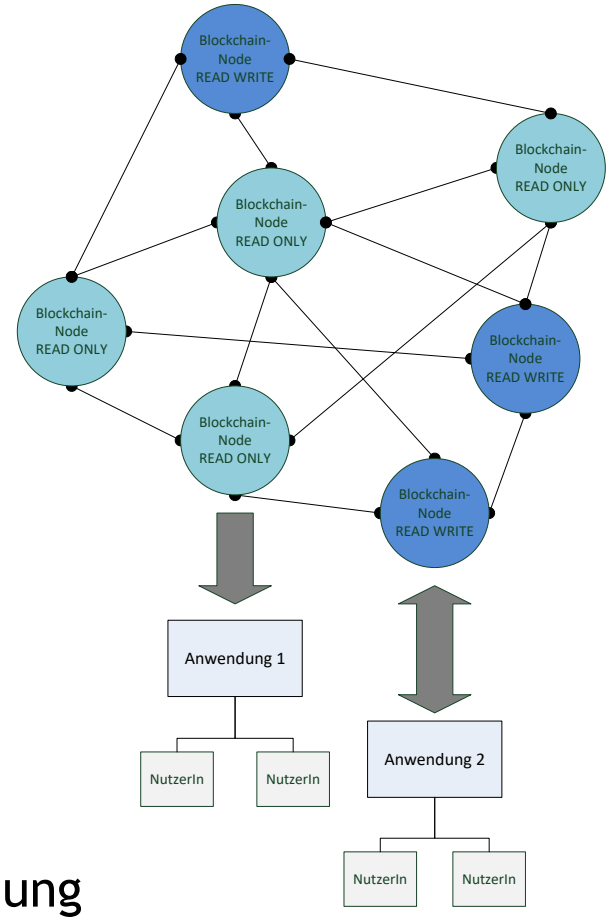
- Initiative von Institutionen der öffentlichen Verwaltung
- „Konsortium-Blockchain“ für unterschiedliche Usecases im „public service“ Bereich
  - Blockchain in Echtbetrieb seit 10/2019
- Konsortialpartner derzeit
  - WKO (Wirtschaftskammer) – Daten-Zertifizierung
  - WU Wien –Notarisierung
  - Stadt Wien – OGD Notarisierung
  - BRZ (Bundesrechenzentrum)
  - Nic.at (cert.at)
- Zugesagt
  - Kontrollbank
- Weitere (angefragt)
  - FH St. Pölten, TU Wien …

Austrian Public Sector Blockchain (Nodes)	Node Test	**Node Produktiv**
BRZ (Bundesrechenzentrum)	ja (2)	**ja (2)**
Stadt Wien - MA01	ja (2)	**ja**
WKO (Wirtschaftskammer Östrerreich)	ja	**ja**
nic.at/cert.at	ja	**ja**
WU (Wirtschaftsuniversität Wien)	ja	**ja**
AUSTRIAPRO	(ja)	

AUSTRIA PRO

Austrian Public Service Blockchain (APSB) Vereinbarung

- Inhalt (**neue Version 0.9**)
  - 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



AUSTRIA PRO

APSB – Status und News

- Vereinbarung liegt in Version 0.9 vor
- Neues Dokument „Leitfaden“
  - Standards und Empfehlungen
  - Für österr. Verwaltungen, die Knoten und darauf basierende Anwendungen betreiben
- Nächste Runde Mitte Oktober
  - Policy fertigstellen
- **Ziel 12/2021: Finales Dokument am e-Government Reference Server**

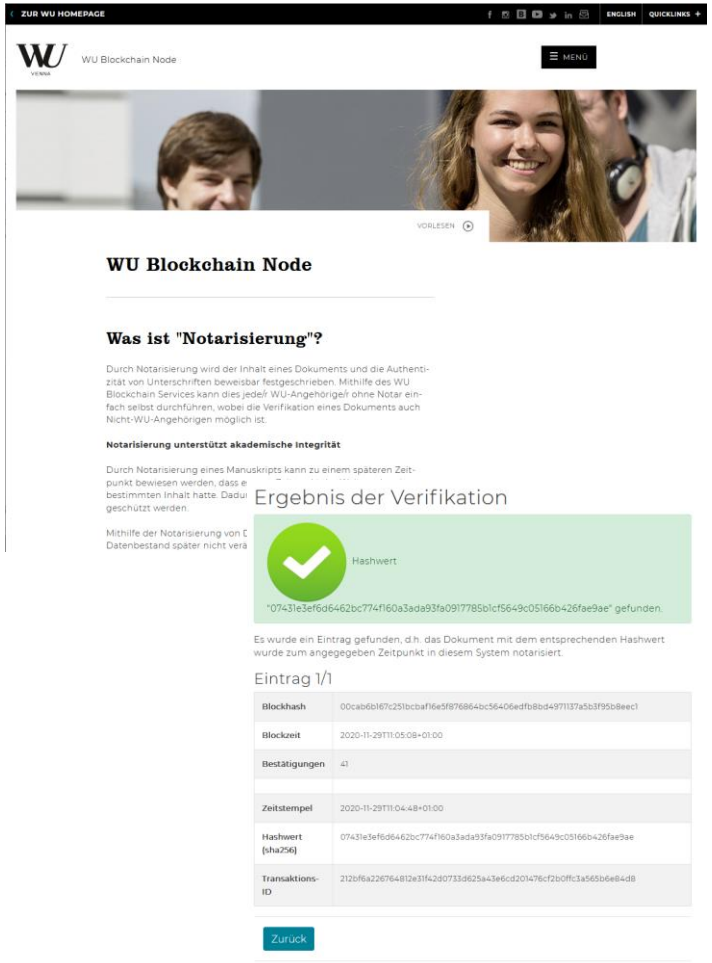
- WKO: Gespräche mit BMDW im Laufen
- Überlegungen hinsichtlich gemeinsamer Wartung & Weiterentwicklung

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

AUSTRIA PRO

APSB – WU (Wirtschaftsuniversität Wien)

- 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 (auch ohne Amtssignatur)
- Organisatorisches
  - Notarisierung erstellen – nur aus WU internem Netz (bzw. VPN)
  - Notarisierung verifizieren – auch aus öffentlichem Netz



APSB – WU (Wirtschaftsuniversität Wien)

- **Neuer Usecase (in Ausarbeitung)**
  - Institut für Produktionsmanagement
  - LVAs für Geschäftsprozesse, Logistik, ERP
- **„SAP-Zertifikate“**
  - Parallel zu LVA-Zeugnis
  - Etabliert als „Qualitätssiegel“
  - Dzt. ca. 60/Semester
  - Zertifikate auf Papier und elektronisch
- **Neu: In Vorbereitung: Kombination Blockchain-Notarisierung + digitale Signatur**

- Auch als Beispiel für andere Institute/Anwendungsfälle

AUSTRIA PRO

„Daten-Zertifizierung“ für die Privatwirtschaft

- Initiative "Private Sector Blockchain"
- AUSTRIAPRO (WKO)
  - „Unterstützung einer privaten Konsortialblockchain zur Zertifizierung von Daten”
  - Zielsetzung: Aufbau einer dauerhaften und sicheren Blockchain-Infrastruktur für Österreichs Wirtschaft
  - Einrichtung und Moderation eines offenen Stakeholder-Forums zum Aufbau und Steuerung der Infrastruktur
    - Kooperation ABC (Austrian Blockchain Center) und AustriaPro (WKO) - Forschungsprojekt
    - Empfehlung **Rechtsform für Konsortium => Verein**

AUSTRIA PRO

BCI

Blockchain Initiative Austria

- „Blockchain Initiative Austria“
  - Offiziell gegründet 1/2021
  - https://www.bc-init.at/
    - Systembeschreibung & Rahmenbedingungen, Spezifikation Datenstruktur …
    - Vereinsstatuten, Beitrittsantrag
- Aktuell (9/2021)
  - 15 Mitglieder & 1 Netzwerkpartner
  - Neu
    - Algordanza Erinnerungsdiamanten GmbH
    - Kosch & Partner Rechtsanwälte GmbH

AUSTRIA PRO

Aktuelle Mitgliederliste

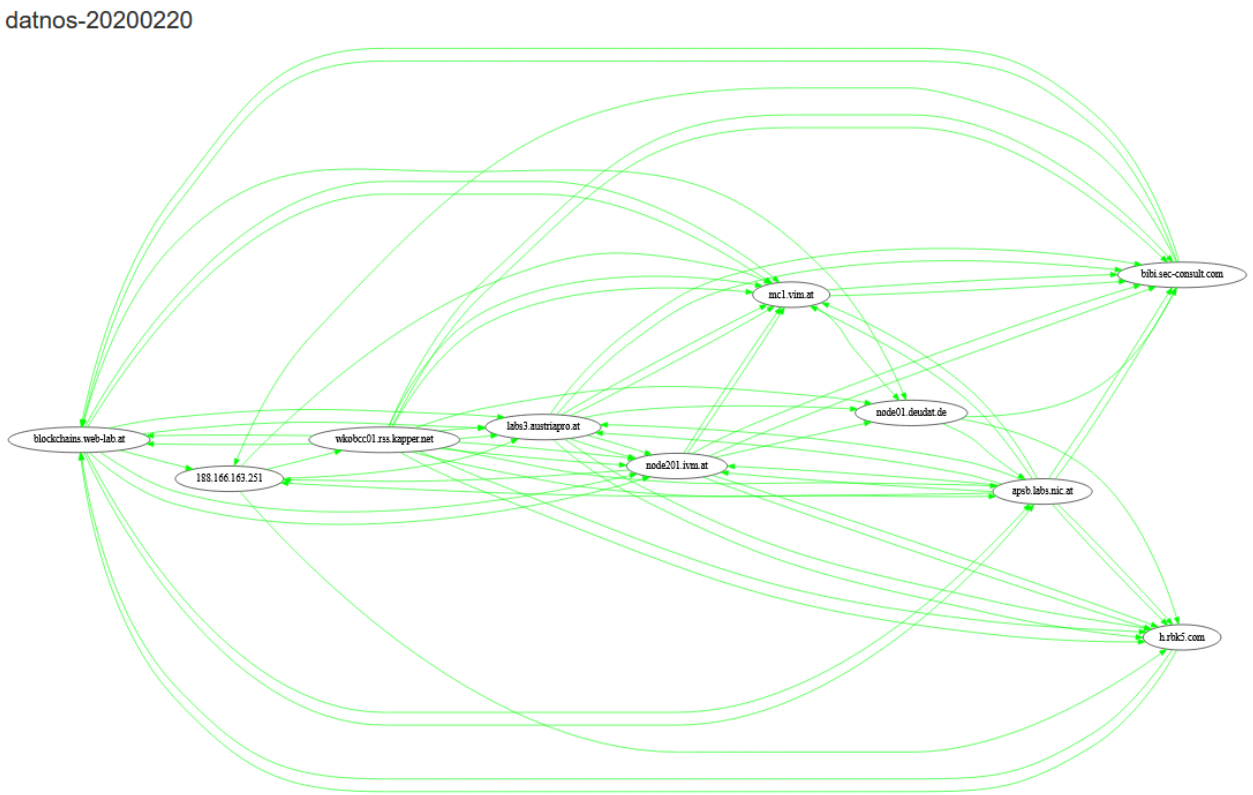
Algordanza Erinnerungsdiamanten Handels GmbH	ALGORDANZA
AUSTRIAPRO - Verein zur Förderung standardkonformer E-Business Lösungen	AUSTRIA PRO
baumann.at - Blockchain Consulting & Development	baumann.at concepts & solutions
DEUDAT GmbH - Datenschutz und Informationssicherheit - Anwendung: Notarisierung	DEUDAT Datenschutz und Informationssicherheit
Infinite Trust Digital GmbH	
IoT Austria - The Austrian Internet of Things Network	IoT AUSTRIA
IVM Technical Consultants GmbH	IVM www.ivm.at
Kosch & Partner Rechtsanwälte GmbH	KOSCH & PARTNER RECHTSANWÄLTE
RBK5 - Dipl.-Ing. Roman Bruckberger-Koch	RBK5
SEC Consult Unternehmensberatung GmbH - Anwendung: ForensicForever	SEC Consult
Securikatt Ulrich & Horn GmbH	SECURIKETT
SIMTOOLS GmbH	SIMTOOLS
SYNERCON GmbH	SYNERCON
VIM Internetdienstleistungen GmbH	VIM IT SOLUTIONS
Woschitz group GmbH	WOSCHITZ GROUP

Ehrenmitglieder

Prof. Alfred Taudes - Institute for production engineering & Research Institute for Cryptoeconomics - WU Wien	WU INTERDISCIPLINARY RESEARCH INSTITUTE FOR CRYPTOECONOMICS

Blockchain & Echtbetrieb

- Blockchain in Echtbetrieb seit 20.2.2020
  - Aktuell 11 Knoten
- Erster Use-Case: „Daten-Zertifizierung“
- **4** Anwendungen in Echtbetrieb
  - Dokumenten-Notarisierung „proof.li“
  - SEC Consult „ForensicForever“
  - DEUDAT.de - Notarisierung
  - **Neu: „Digitale Zertifizierung von Kosch & Partner RA GmbH“**
    - https://digicert.kosch-partner.at



„proof.li“

- Dokumenten-Notarisierung
  - Im Echtbetrieb
  - Referenzimplementierung
- Nutzung von „Vouchers“
  - Vergeben vom Verein
  - **an „friendly user“**
  - hello@bc-init.at
- Features
  - Einfache, anonyme Nutzung
  - Keine Registrierung, kein Login …

AUSTRIA PRO

Weitere News der „Blockchain Initiative Austria“

Gutachten in Erstellung

- Analog zu bestehenden Gutachten (APSB)
- Fokus „Private Sector Blockchain“
- Rahmenbedingungen für den Aufbau und Betrieb der durch die Vereinsmitglieder betriebenen Konsortium-Blockchain

Planung Generalversammlung

- Mitte November 2021
- Programm lt. Statuten
- Persönliche Vorstellung der Mitglieder
- Abstimmung nächste Schritte/Aktionen/Synergien

"Daten-Zertifizierung" auf Basis Blockchain - Gutachten

- Privatgutachterliche Stellungnahme
  - Dr. Knasmüller (allg. beeideter & ger. zertif. Sachverständiger)
- Inhalt
  - Beschreibung System und Funktionsweise
  - Verwendete Technologien & Standards
- Publiziert am 6.3.2020 - https://www.wko.at/service/netzwerke/gutachten-daten-zertifizierung-auf-basis-blockchain.pdf

Zusammenfassung:

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

AUSTRIA PRO

News aus dem TestLab

- Node für ABC-Projekt „CPSC“

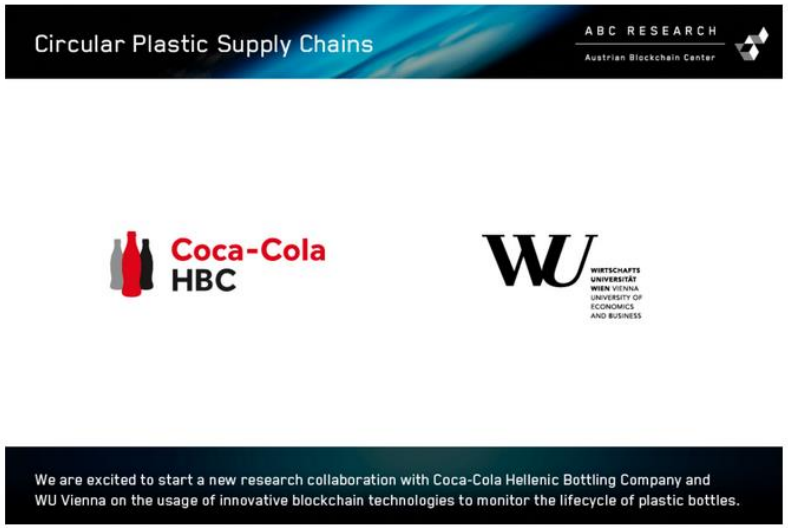
- Aktuelle AustriaPro-Projekte
  - Zeugnisse
  - Tokenisierung Devices
  - Identifikation Devices

- Überarbeitung Info-Unterlagen
  - Notarisierung Ablauf
  - Smart Contracts „Purchase“

AUSTRIA PRO

Node für ABC-Projekt „CPSC“

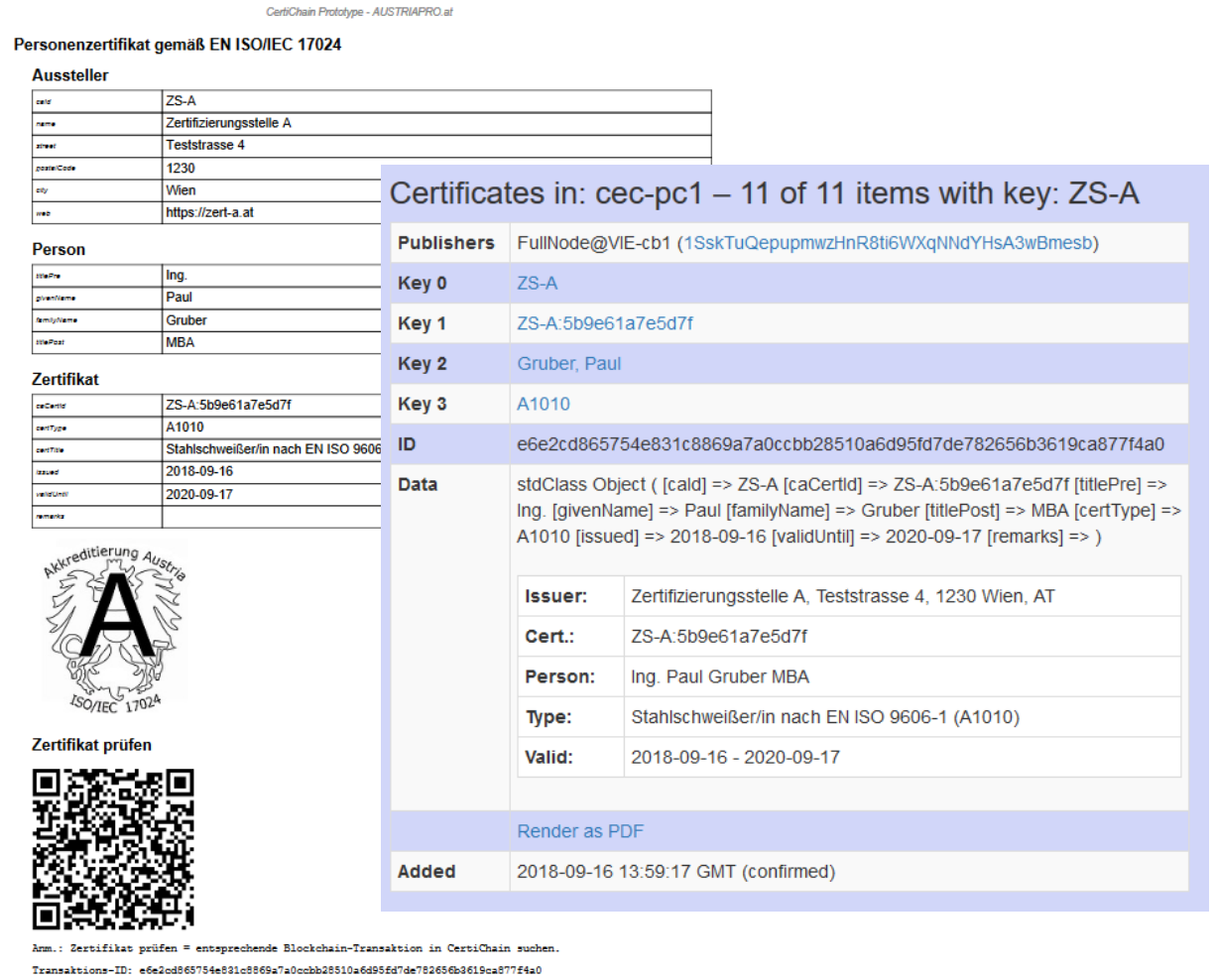
- Projekt „Circular Plastic Supply Chain“
- WU & ABC
- https://www.abc-research.at/new-project-circular-plastic-supply-chains/
- Einsatz von Blockchain-basierten Anreizen auf das Recyclingverhalten
  - Sammeln und Recyclen von PET Flaschen
  - Scannen von QR-Codes
  - Belohnung durch „Reward-Tokens“
- Private Konsortium-Blockchain
  - AustriaPro stellt einen der Nodes



AUSTRIA PRO

Projekt „Zeugnisse“

- Basierend auf den Vorarbeiten (Projekt „Personenzertifikate“)
- Zeugnisse (z.B. Lehrlinge, Meisterprüfung)
- Schnittstellen zu WKO Systemen
- Phase 1: Prototyp im BC-Lab „Klick-Dummy“
- Phase 2: Testsystem



CertiChain Prototype - AUSTRIAPRO.at

Personenzertifikat gemäß EN ISO/IEC 17024

Aussteller

caId	ZS-A
name	Zertifizierungsstelle A
street	Teststrasse 4
postalCode	1230
city	Wien
web	https://zert-a.at

Person

titlePre	Ing.
givenName	Paul
familyName	Gruber
titlePost	MBA

Zertifikat

caCertId	ZS-A:5b9e61a7e5d7f
certType	A1010
certTitle	Stahlschweißer/in nach EN ISO 9606
issued	2018-09-16
validUntil	2020-09-17
remarks	

Akkreditierung Austria A ISO/IEC 17024

Zertifikat prüfen

Anm.: Zertifikat prüfen = entsprechende Blockchain-Transaktion in CertiChain suchen.

Transaktions-ID: e6e2cd865754e831c8869a7a0ccbb28510a6d95fd7de782656b3619ca877f4a0

Certificates in: cec-pc1 – 11 of 11 items with key: ZS-A

Publishers	FullNode@VIE-cb1 (1SskTuQepupmwzHnR8ti6WXqNNdYHsA3wBmesb)
Key 0	ZS-A
Key 1	ZS-A:5b9e61a7e5d7f
Key 2	Gruber, Paul
Key 3	A1010
ID	e6e2cd865754e831c8869a7a0ccbb28510a6d95fd7de782656b3619ca877f4a0
Data	stdClass Object ([cald] => ZS-A [caCertId] => ZS-A:5b9e61a7e5d7f [titlePre] => Ing. [givenName] => Paul [familyName] => Gruber [titlePost] => MBA [certType] => A1010 [issued] => 2018-09-16 [validUntil] => 2020-09-17 [remarks] =>)
	Render as PDF
Added	2018-09-16 13:59:17 GMT (confirmed)

Issuer:	Zertifizierungsstelle A, Teststrasse 4, 1230 Wien, AT
Cert.:	ZS-A:5b9e61a7e5d7f
Person:	Ing. Paul Gruber MBA
Type:	Stahlschweißer/in nach EN ISO 9606-1 (A1010)
Valid:	2018-09-16 - 2020-09-17

Projekt „Tokenisierung und Identifikation von Devices “

- Abbildung von Devices mit NFTs
  - Kessel
  - Kühlanlagen
  - …
- Dokumentation Eigentümer & Wartungen
- Identifikation und Absicherung der Daten mit „Secure Elements“
- Status: Grobplanung, Vorbereitungen

- -> Überblick/Einleitung NFTs

AUSTRIA PRO

NFTs: „Non fungible Tokens“

- Fungible: „replaceable by another identical item; mutually interchangeable”
  - „beliebig austauschbar“
  - Beispiel: Euro Münze
- Non fungible: „unique and cannot be replicated or replaced with anything else”
  - „einmalig“ oder zumindest „eindeutig unterscheidbar“
  - Beispiel: Mona Lisa
- NFTs
  - „Token“ (digital dargestelltes) Objekt auf einer Blockchain
  - Repräsentiert virtuelles oder reales Gut
  - Handelbar, übertragbar
  - In Krypto-Wallets „aufbewahren“

NFT - Anwendungen für …

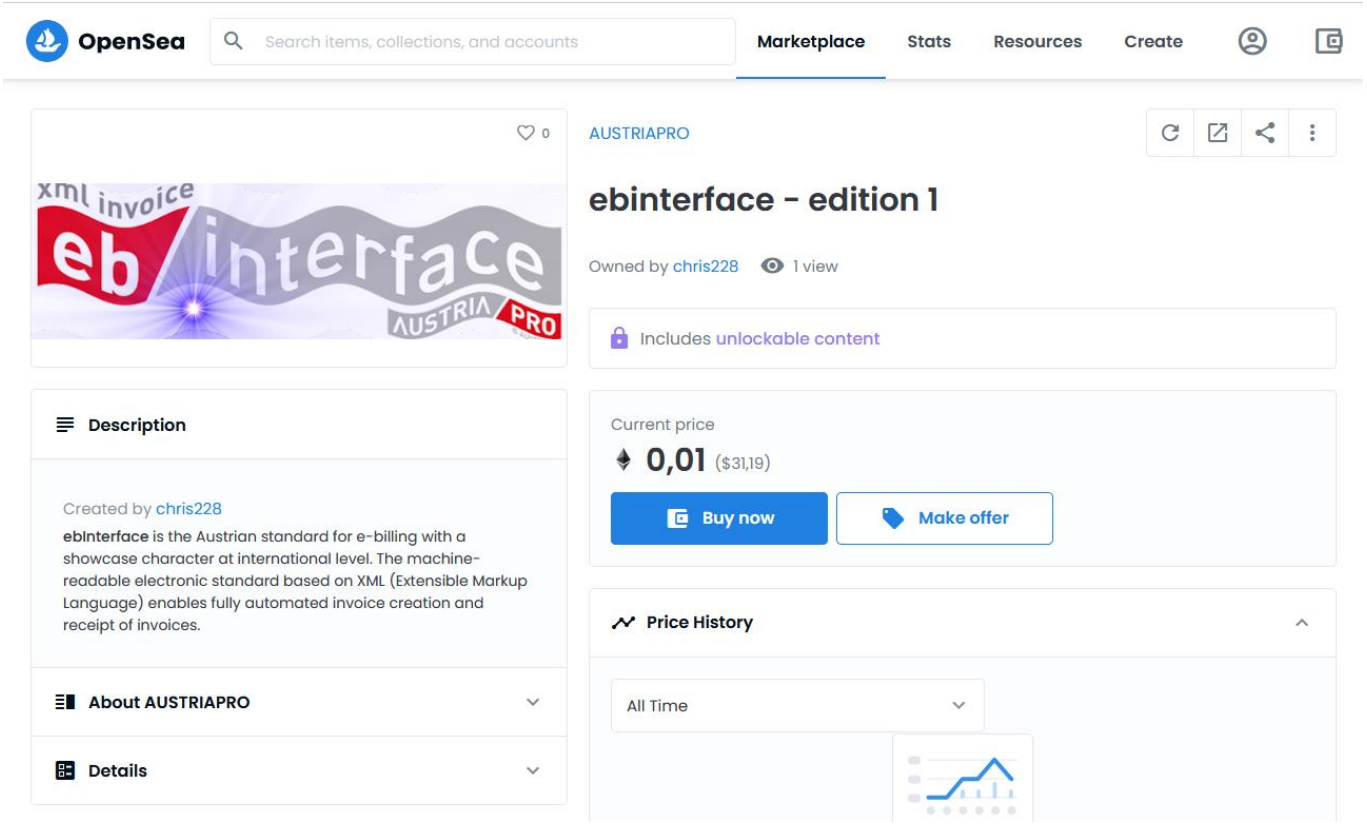
- Virtuelle Objekte
  - Digitale Kunst (Grafik, Video, Musik)
  - Digitale Daten (Sourcecode, Texte …)
  - Objekte in Computerspielen
  - …
- Digitale Zwillinge
  - Konsumgüter
  - Immobilien
  - Mode
  - Briefmarken!
  - …
  - >>> Anlagen <<<

AUSTRIA PRO

Aktuelle Beispiele

- KryptoKitties „Das erste große Blockchain Spiel“
  - Virtuelle Katzen sammeln, züchten & handeln
  - Start Ende 2017, bis zu 1,5 Mio User
  - Meist genutzter Smart Contract auf Ethereum
  - Juli 2020: Handelsvolumen von 37 Mio USD
- Sportbereich: Spielerkarten (FC Bayern, NBA), Rennautos …
- Mode: Nike NFT-Schuh …
- Social Media: Tweets, Sourcecode …
- Virtuelles Land: Decentraland, Metaversum …
- Kunst!
  - Bereits 10% von weltweitem Umsatz im Kunstmarkt
  - 1 HJ 2021: 2,5 Milliarden USD

AUSTRIAPRO ebinterface als NFT „Kunst“



https://opensea.io/assets/0x495f947276749ce646f68ac8c248420045cb7b5e/115396737687183052340650093407955369796263433278523039622569928946111425282049

AUSTRIA PRO

NFTs - Blockchain

- Auf Blockchain gespeichert
  - „existieren ewig“ (im Ggs zu firmenspezifischen Systemen)
  - Aktueller Eigentümer klar (Walletadresse)
  - Auf (dezentralen) Börsen handelbar
- Übliche Platform: Ethereum -> Probleme
  - Teilweise überlastet -> teure Transaktionsgebühren
  - Smart Contracts: „Minting“ und Transferieren -> Proof Of Work (rechenintensiv, Stromverbrauch, CO2 …)
  - Ethereum 2.0 (Proof Of Stake) - Skalierung und Stromverbrauch keine Probleme mehr

Industrielle Anwendungen

- NFT als „Digitaler Zwilling“ von Produkten (z.B. Anlagen)
- Koppelung über digitale Identität (Secure Element)
- Funktionen
  - Eindeutige ID der Anlage
  - Jeweils aktueller Eigentümer definiert
  - Zusatzinformationen eindeutig zuzuordnen
    - Z.B. Dokumentation der Wartung
  - Komplette Historie (Eigentümer, Dokumentation …) unveränderbar in Blockchain abgelegt

- Beispiele (AustriaPro Projekt?)
  - Klimaanlagen
  - Waagen
  - …

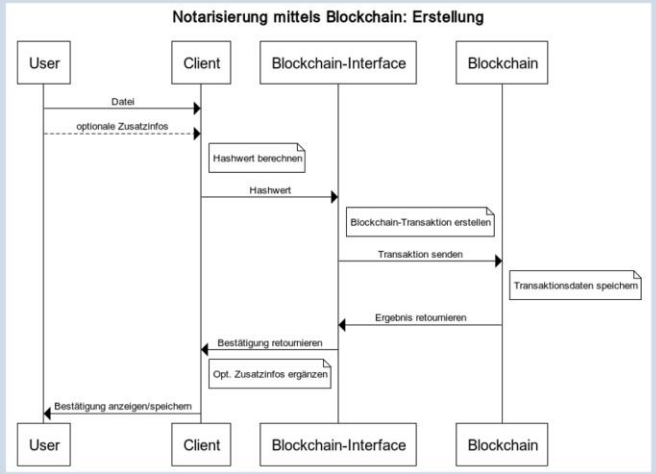
AUSTRIA PRO

Secure Element

- Crypto-Chip
  - integriert in „Device“
    - Maschine, Anlage, Sensor …
    - auch z.B. Smartphone oder Teil einer SIM Karte
- Funktionen
  - Generierung von Schlüsselpaaren
    - Private Key nicht (zerstörungsfrei) auslesbar
  - Identität (Public Key)
  - Verschlüsselung
  - Digitale Signatur

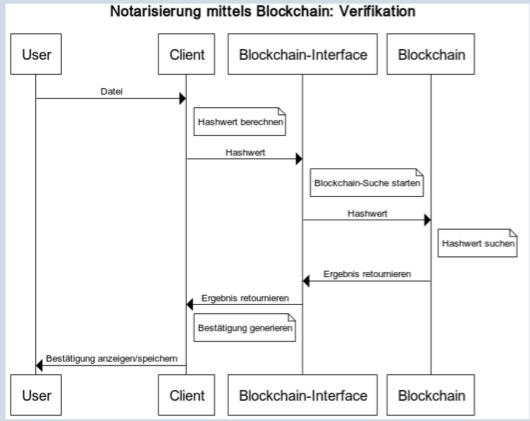
Überarbeitung Info-Unterlagen (Notarisierung)

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.“

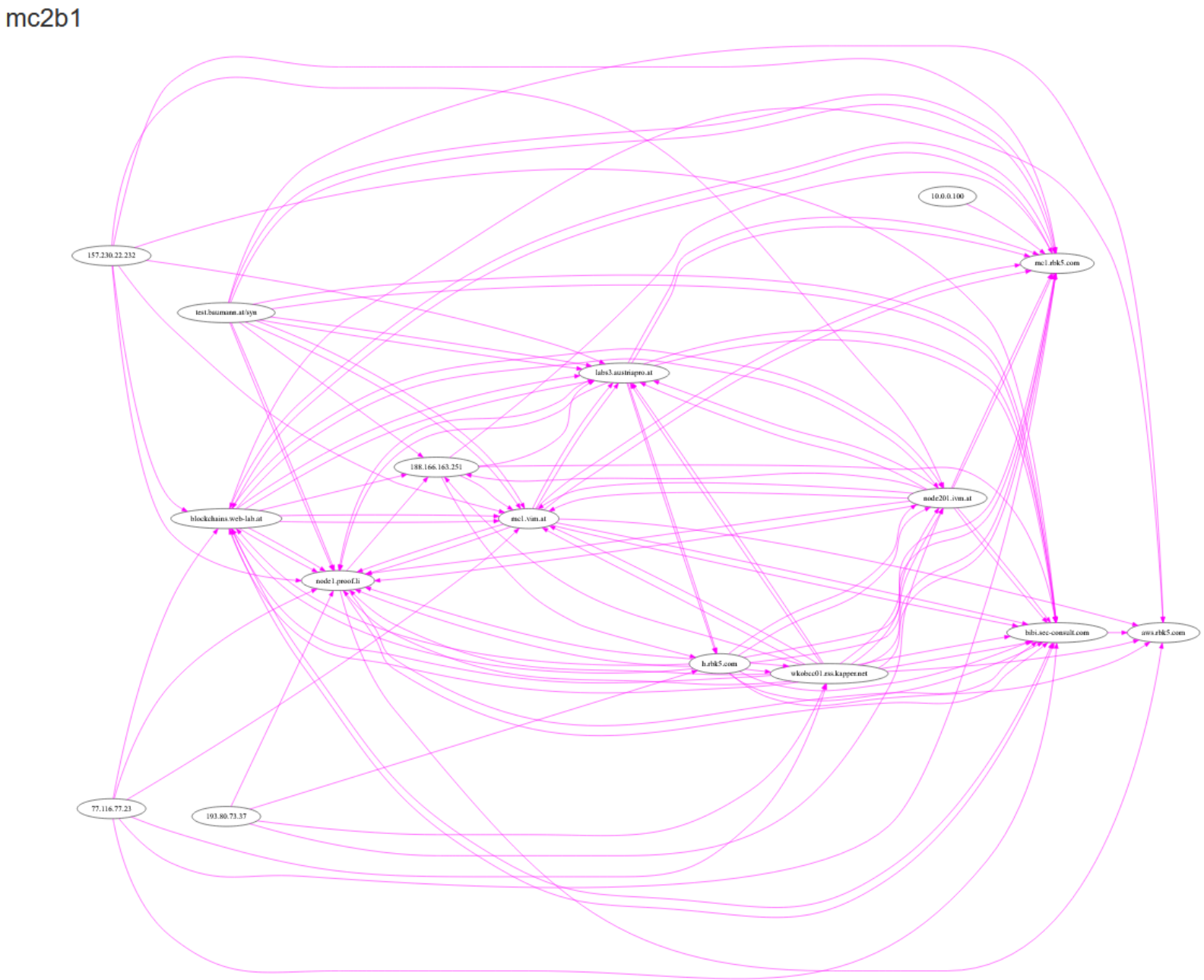
AUSTRIA PRO

Überarbeitung Info-Unterlagen (Smart Contracts)

Smart Contracts - Beispiel „Purchase“

```
contract Purchase {
    uint public value;
    address public seller;
    address public buyer;
    enum State { Created, Locked, Inactive }
    State public state;

// Seller muss doppelten Verkaufspreis (value) "hinterlegen"
    function Purchase() payable {
        seller = msg.sender;
        value = msg.value / 2;
        if (2 * value != msg.value) throw;
    }

// Buyer bestätigt das Angebot
// und muss ebenfalls doppelten VK-Preis hinterlegen
// Contract wird auf Status "locked" gesetzt
    function confirmPurchase()
        inState(State.Created)
        require(msg.value == 2 * value)
        payable
    {
        purchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }

// Seller sendet Ware an Buyer
// Buyer bestätigt Erhalt der Ware
// die gelockten Beträge werden freigegeben
    function confirmReceived()
        onlyBuyer
        inState(State.Locked)
    {
        itemReceived();
        state = State.Inactive;
// Buyer erhält 1 x Wert zurück
// Seller den Rest: 3 x Wert (2 x sein Deposit, 1 x Verkaufspreis)
        if (!buyer.send(value) || !seller.send(this.balance))
            throw;
    }


// Seller kann Contract stornieren, solange er noch nicht
// confirmed wurde (state locked)
    function abort()
        onlySeller
        inState(State.Created)
    {
        aborted();
        state = State.Inactive;
        if (!seller.send(this.balance))
            throw;
    }
}
```

AUSTRIA PRO



Multichain Test-Netz

- AustriaPro Lab
- & friends

- Diverse Beispiele (Code) verfügbar (github)

- Offen für weitere Teilnehmer

- MITMACHEN!!!

- Vorschau Blockchain Award 2021 und eDay 2021
  - Beurteilung der Einreichungen durch Jury: ongoing
  - Preisverleihung anlässlich eDay 2021 – 7.12.2021 in der WKO

- open space – Projekte, Initiativen, Informationen

Kooperation mit DIO (Data Intelligence Offensive)

AUSTRIA PRO

open space – Projekte, Initiativen, Informationen

- „Digitaler Frachtbrief & Blockchain“, Alex Schaefer, editel
- weitere Meldungen (spontan)

Vielen Dank für Ihre Aufmerksamkeit.

www.austriapro.at

austriapro@wko.at

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