Arbeitskreis Blockchain
Arbeitsgruppe Technik & Blockchain Lab

AUSTRIAPRO

Dr. Christian Baumann

4.9.2019

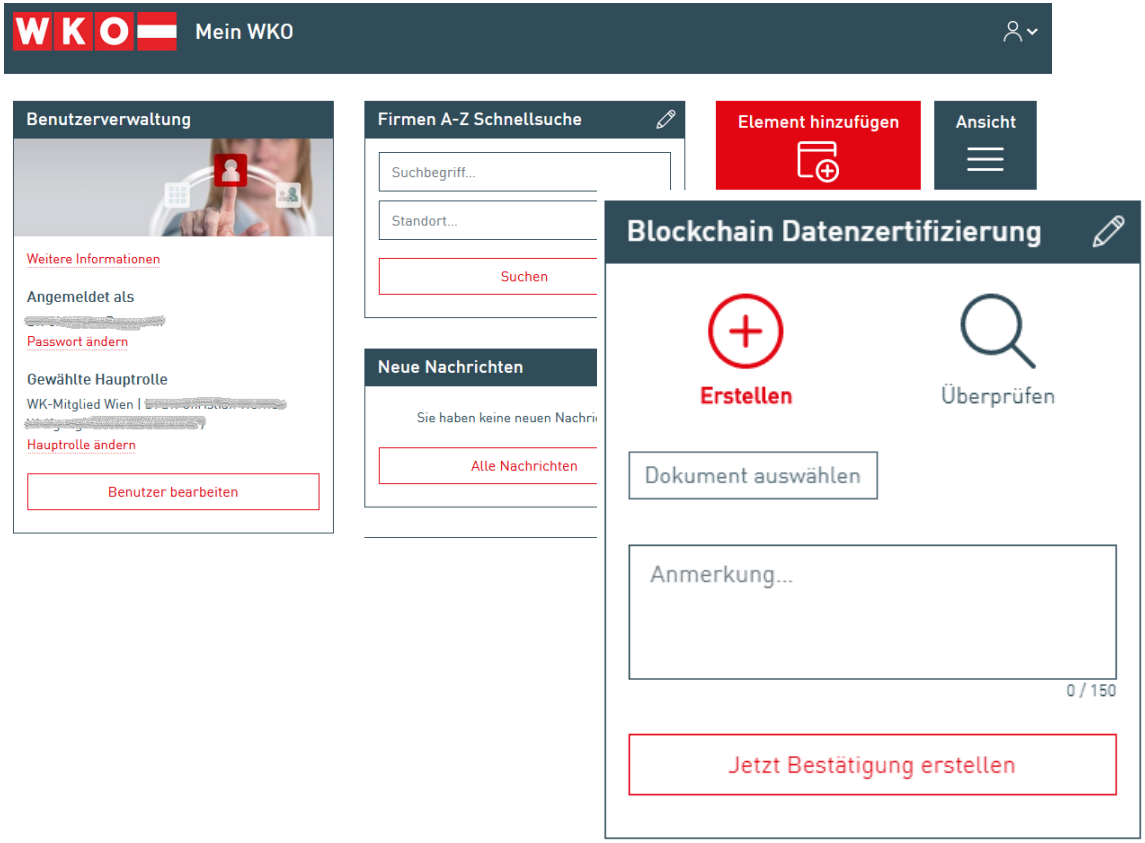
Agenda

- Allgemein
  - Blockchain Offensive der WKÖ
  - Status „Datenzertifizierung“ (WKÖ und privat)
  - Gutachten „Daten Zertifizierung auf Basis Blockchain“
- Blockchain-Lab
  - CPB: Ethereum Demo Projekt
  - Programmierung/Praxis
  - Speed/Size
  - Blockchain & DSGVO
- Zertifizierung
  - „personal certificates on blockchain“ - Marvin Hölzl

Blockchain Offensive der WKÖ

- => siehe eigene Präsentation

Dashboard „mein.wko.at“



WIRTSCHAFTSKAMMER ÖSTERREICH

Blockchain Datenzertifizierung - Bestätigung

Erstellt am 29.07.2019 um 23:06:32 Uhr

Zum angegebenen Zeitpunkt wurde der Hashwert eines Dokumentes in der Blockchain hinterlegt.

Details zum hinterlegten Dokument:

Dateiname	geparden 3sat(25-01-10 21-20-43).mpg
Hashwert	992d34a1eaaf26a41a20b2a4c70b82671349a92a2f231b425ccfabdc22fbf17c
Anmerkung	Videodreh Rihafilm Südafrika
Transaktions-ID	618882c2c82ebc45d4ce532f8b0c83bb047e8d6be6490ee08a0e33d658da9333

Sie können die Transaktions-ID mit folgendem QR-Code bzw. Link an ein Verifikationsservice übergeben.

https://blockchains.web-lab.at/docnos/?page=verify&oid=618882c2c82ebc45d4ce532f8b0c83bb047e8d6be6490ee08a0e33d658da9333

Bitte beachten: Das System ist derzeit im Testbetrieb!

Status „Daten-Zertifizierung“ WKO

- Blockchainumgebung (Node Echtsystem) betriebsbereit & gekoppelt mit BRZ und Wien
  - VPN
  - Blockchains (Test & Echt)
- Integration GUI in mein.wko: ongoing, geplante Fertigstellung 10/2019
- Festlegung diverser Details mit BRZ: Herbst 2019
  - Benennung Chains, Streams
  - Rollierung
  - …

„Datenzertifizierung“ für die Privatwirtschaft

- Bereits mehrere Anfragen aus Privatwirtschaft
- 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
  - Bei AustriaPro, weil auch für nicht-WKO-Mitglieder
  - WKO betreibt Blockchain-Knoten (aktuell Testsystem)

„Datenzertifizierung“ für die Privatwirtschaft

- 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 für „Mitglieder des Konsortiums“
    - Öffentlicher Lesezugriff (Read-Only Nodes) zum Validieren der Daten
- Zeithorizont
  - Testsystem ab sofort (Blockchain-Lab)
    - Ein paar Unternehmen betreiben bereits Test-Nodes
    - => Technisch konsolidieren
  - Echtsystem? Tbd.

"Daten Zertifizierung" auf Basis Blockchain - Gutachten

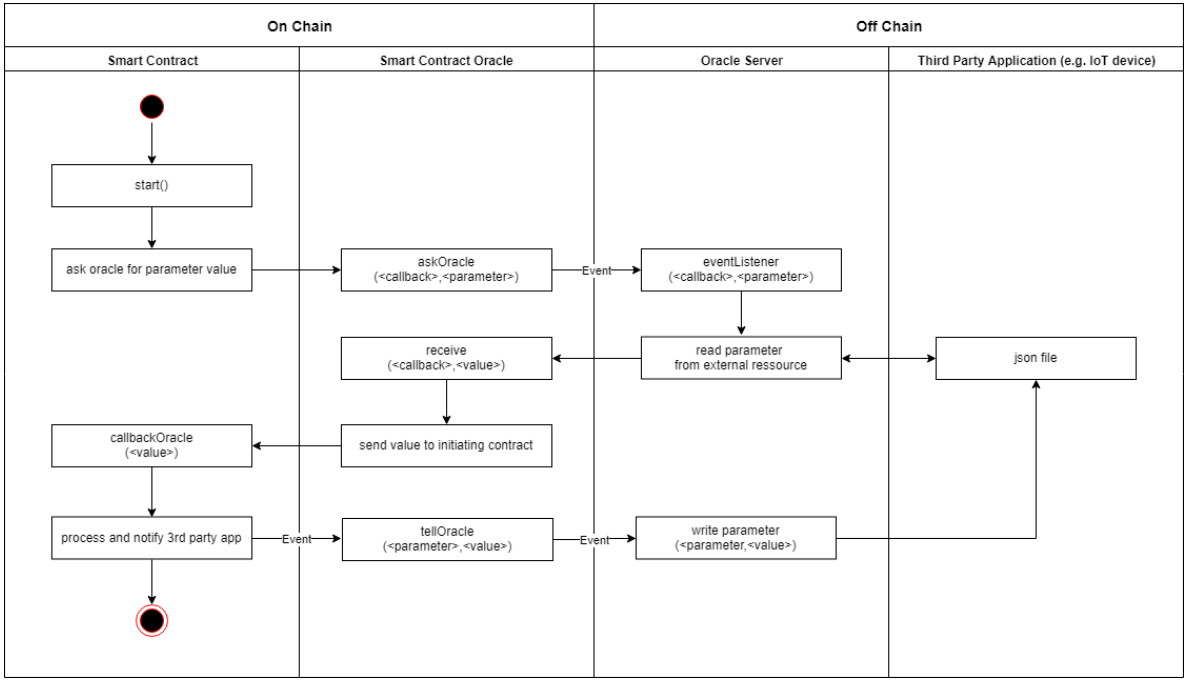
- Privatgutachterliche Stellungnahme
  - Dr. Knasmüller (allg. beeideter & ger. zertif. SV)
- Geplanter Inhalt
  - Beschreibung System und Funktionsweise
    - zB. lt. https://blockchains.web-lab.at/docnos/ (Testsystem von WKO Daten Zertifizierung)
  - Verwendete Technologien & Standards
    - Multichain; Opensource ...
    - Hashwertberechnungen lt. mindestens SHA-2/256 oder SHA-3
  - Praktische Versuche
    - im Rahmen des AUSTRIAPRO Blockchain Labs
  - Ggf. Verbesserungsvorschläge
    - "Verständnis"

Phase 6: Ethereum V2

- Schwerpunkte
  - Smart Contracts
  - Oracles
- Aktualisierung Labs-Ethereum Plattform
  - Parity Ethereum https://www.parity.io/
  - Dokumentation für Setup von „Proof Of Authority" Chains
  - Weiterer Server https://labs2.austriapro.at/
- Ausblick
  - „Polkadot": Next generation platform für connection independent blockchains ...

Phase 6: Ethereum Demo Projekt

- Smart Contracts & Oracles
  - Oracles (bidirektional)
  - Einfache Datenhaltung



Ethereum Demo Projekt

- => siehe Präsentation Fa. CPB

Blockchain-Lab: Programmierung/Praxis

- Daten in/aus Blockchain schreiben/lesen
- Am Beispiel Multichain Streams
  - Daten in JSON
  - Datenfelder & Hashwert
  - für z.B. „Daten Zertifizierung“
  - Incl. Fehlerhandling, Abfrage Blockchaininfos etc.
- Sourcecode auf Github
  - https://github.com/austriapro/blockchain/tree/master/multichain-samples

Blockchain-Lab: Programmierung/Praxis

```php
<?php
/**********************************************************************************
AUSTRIAPRO Blockchain Lab - Demo

Write data to Blockchain (Multichain) stream

8/2019
C. Baumann - AUSTRIAPRO
**********************************************************************************/

require_once('config.php');
require_once('multichain-api.php');

// initialize RPC connection to Multichain Instance
$chain = new MultiChain($cfg->rpcUser, $cfg->rpcPass, $cfg->rpcHost, $cfg->rpcPort);

class cData{};
$data = new cData();
$timeStamp = date('c');
$data->timeStamp = $timeStamp;
$data->client = $cfg->client;

$clientData = new cData();
$clientData->name = 'some Name';
$value = rand(0, 100);
$clientData->value = $value;
$clientData->hash = 'sha256:' . hash('sha256', $value);
$clientData->remark = 'some remark for value ' . $value;

$data->data = $clientData;

// prepare to publish in JSON mode
$dataToPublish = array('json' => $data);

// show data to be published
var_dump($dataToPublish);
```

Stream: stream3 – 106 of 106 items

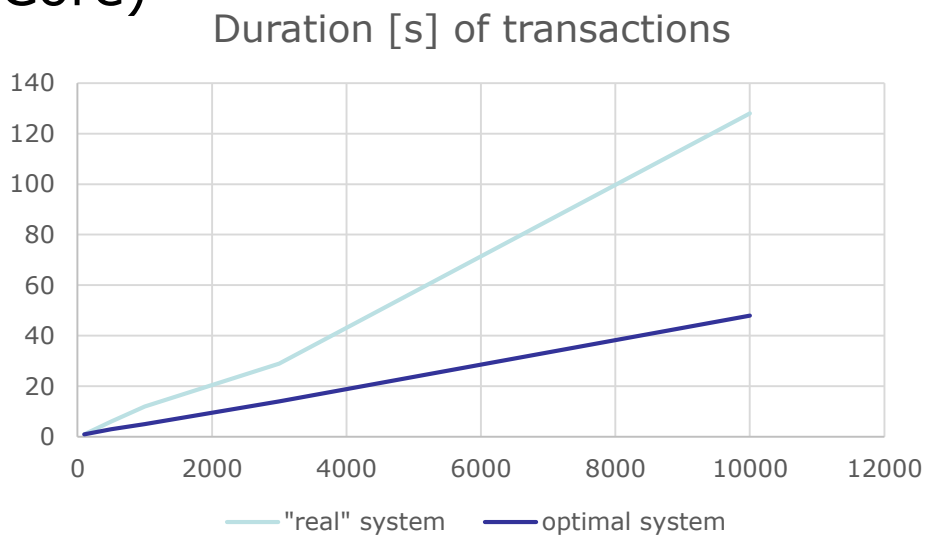
Publishers	1Jf8ESNf3qWMJbAY7jwDax4YM3WZYvybv8NZ6M
Key 0	AP-key-1
Key 1	another key

JSON data	<pre>{
	"timeStamp": "2019-08-30T12:03:27+02:00",
	"client": "AustriaPro Lab Client 1",
	"data": {
	"name": "some Name",
	"value": 95,
	"hash": "sha256:ad48ff99415b2f007dc35b7eb553fd1eb35ebfa2f2f308acd9488e
	"remark": "some remark for value 95"
	}
	}</pre>

Added	2019-08-30 10:03:38 GMT (confirmed)
Data location	on-chain, available

Blockchain-Lab: Speed/Size

- Transaktionen pro Zeit
  - Items in Streams speichern, ca. 1 kByte/Item
  - „Real“: REST-API, Webservice
  - „Optimal“: Script, schreibt direkt in Blockchain
  - (Angaben pro Node/Core)



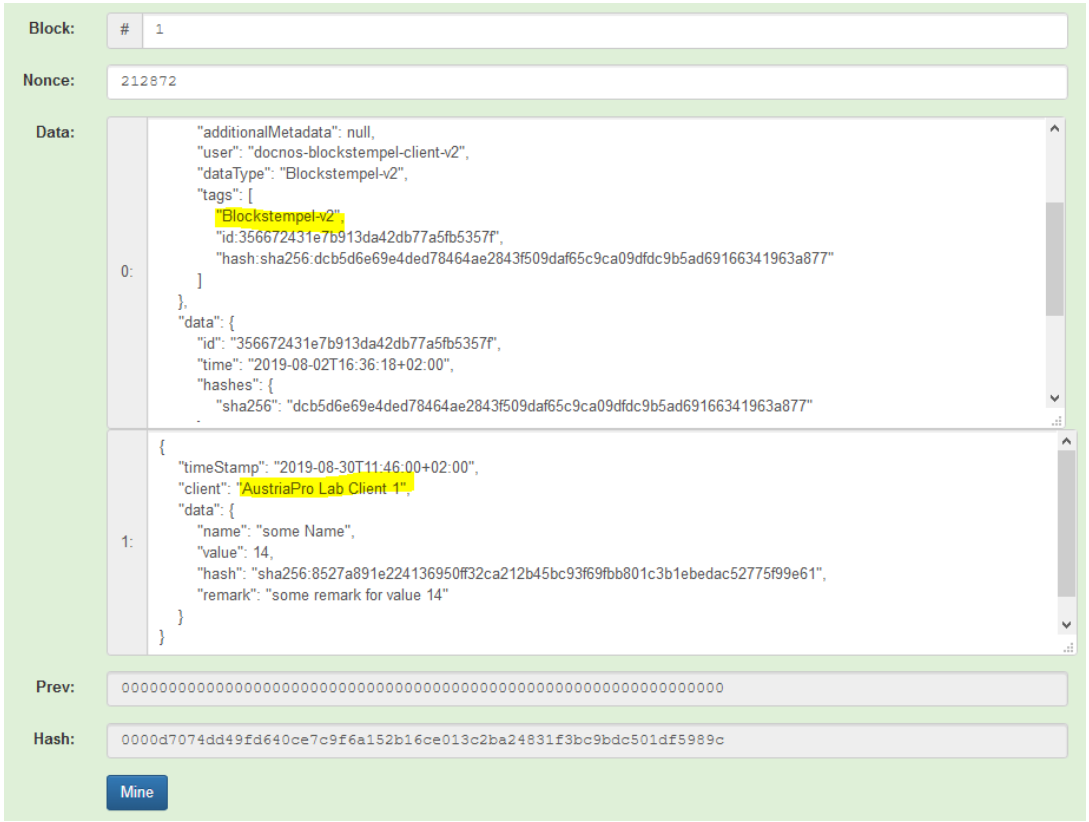
Blockchain-Lab: Speed/Size

- Speicherbedarf
  - Beispiel Air Quality Chain (Multichain)
  - ca. 18 Monate in Betrieb

Example: Air Quality Chain					
Stream	**Items**	**avg. Size**	**Size [Bytes]**		**Average [Bytes]**
wien	448 949	150	67 342 350		
rad-oe	9 638	7 350	70 839 300		
ozon-oe	1 072 544	346	371 100 224		
noe	35 360	160	5 657 600		
noe2	53 298	160	8 527 680		
Sum	**1 619 789**		**523 467 154**		**323**
Size on disk					
./blocks			1.3G		
./blocks/index			178M		
./chainstate			1.9M		
./database			16K		
./entities.db			6.0M		
./permissions.db			74M		
./wallet			107M		
./wallet/txs.db			63M		
Total			**1.6G**		**1012**

Blockchain-Lab: Blockchain Demo

- Weiterer Beispielblock (Daten-Zertifizierung)



Blockchain-Lab: Blockchain & DSGVO

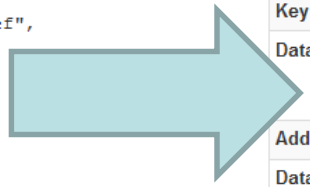
- Diskrepanz
  - Blockchains: „Daten nicht löschbar …“ (Immutability)
  - DSGVO Art. 17: „Recht auf Vergessenwerden …“
- Beispiel: Personenzertifikate
  - Vgl. Gutachten Prof. Forgo
- Lösungsansatz
  - Personenbezogene Daten „offchain“ (zB. verteiltes Filesystem, Blockchain Verknüpfung per Link)
  - Nötigenfalls
    - `Offchain Daten löschen („purge“)`
    - `Personenbezug „geht ins Leere“`
  - Andere Daten und Keys bleiben erhalten
  - (ggf. nodeübergreifende Logik mit Bestätigungen)

Offchain data purging – Beispiel (Multichain Enterprise)

Stream: certificates – 2 of 2 items

Publishers	1YJuGmDpXAC7CaxMyo4k8SV8NCXcuhRcC1axJH
Key 0	A1030
Key 1	"ZS-A:5b8e6a8306e03
JSON data	{ "caId": "ZS-A", "caCertId": "ZS-A:5b8e6a8306e03", "titlePre": "", "givenName": "Peter", "familyName": "Erdinger", "titlePost": "", "certType": "A1030", "issued": "2018-09-04", "validUntil": "2020-07-20", "remarks": "" }
Added	2019-09-01 14:20:08 GMT
Data location	off-chain, available

Publishers	1YJuGmDpXAC7CaxMyo4k8SV8NCXcuhRcC1axJH
Key 0	A1010
Key 1	ZS-A:5b4db31a62bef
JSON data	{ "caId": "ZS-A", "caCertId": "ZS-A:5b4db31a62bef", "titlePre": "Ing.", "givenName": "Franziska", "familyName": "Schweiger", "titlePost": "MBA", "certType": "A1010", "issued": "2018-07-17", "validUntil": "2020-07-20", "remarks": "" }
Added	2019-09-01 14:19:11 GMT (confirmed)
Data location	off-chain, available



Stream: certificates – 2 of 2 items

Publishers	1YJuGmDpXAC7CaxMyo4k8SV8NCXcuhRcC1axJH
Key 0	A1030
Key 1	"ZS-A:5b8e6a8306e03
JSON data	{ "caId": "ZS-A", "caCertId": "ZS-A:5b8e6a8306e03", "titlePre": "", "givenName": "Peter", "familyName": "Erdinger", "titlePost": "", "certType": "A1030", "issued": "2018-09-04", "validUntil": "2020-07-20", "remarks": "" }
Added	2019-09-01 14:20:16 GMT (confirmed)
Data location	off-chain, available

Publishers	1YJuGmDpXAC7CaxMyo4k8SV8NCXcuhRcC1axJH
Key 0	A1010
Key 1	ZS-A:5b4db31a62bef
Data	*Not available. Either the data is off-chain and has not yet been delivered, or the data has been erased because of a "right to be forgotten" request according to the General Data Protection Regulation (GDPR) Art. 17.*
Added	2019-09-01 14:19:11 GMT (confirmed)
Data location	off-chain, NOT available

Blockchain Lab – Weitere Themen

- Absicherung von externen Devices mit Hilfe von digitalen Identitäten für diese
  - z.B. für Daten für Oracles für Smart Contracts
  - Vertrauenswürdigkeit von Sensordaten (IoT …)
  - in Kooperation mit dem Arbeitskreis WPV
    - Verwaltung dieser elektronischen Identitäten

- „Anchoring“: Zusätzliche Absicherung von (privaten/Konsortium) Chains mit Hilfe von State-Notarisierung in public Blockchains
  - Incl. prototypischer Implementierung

Zertifizierungen lt. ISO17024

- Thema aufgearbeitet von Marvin Hölzl (MSc)
  - Masterarbeit
  - Schwerpunkt Schweißzertifikate
- Vorstellung der Masterabreit (& Diskussion)
- **„personal certificates on blockchain"**

News

- …

Kontakt

AUSTRIAPRO

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

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