

Arbeitskreis Blockchain

Allgemeines & Arbeitsgruppe Technik & Blockchain Lab

Dr. Christian Baumann

22.6.2021



Agenda

- News zu „Austrian Public Service Blockchain“
- News zu „Datenzertifizierung für die Privatwirtschaft“
- News aus dem TestLab (Anwendungsfälle, technische Fragen)
 - „Technische Erweiterungen für Konsortialblockchains auf Multichain-Basis“
- Vorschau Blockchain Award 2021
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - spontane Beiträge zu Projekten, Initiativen etc.

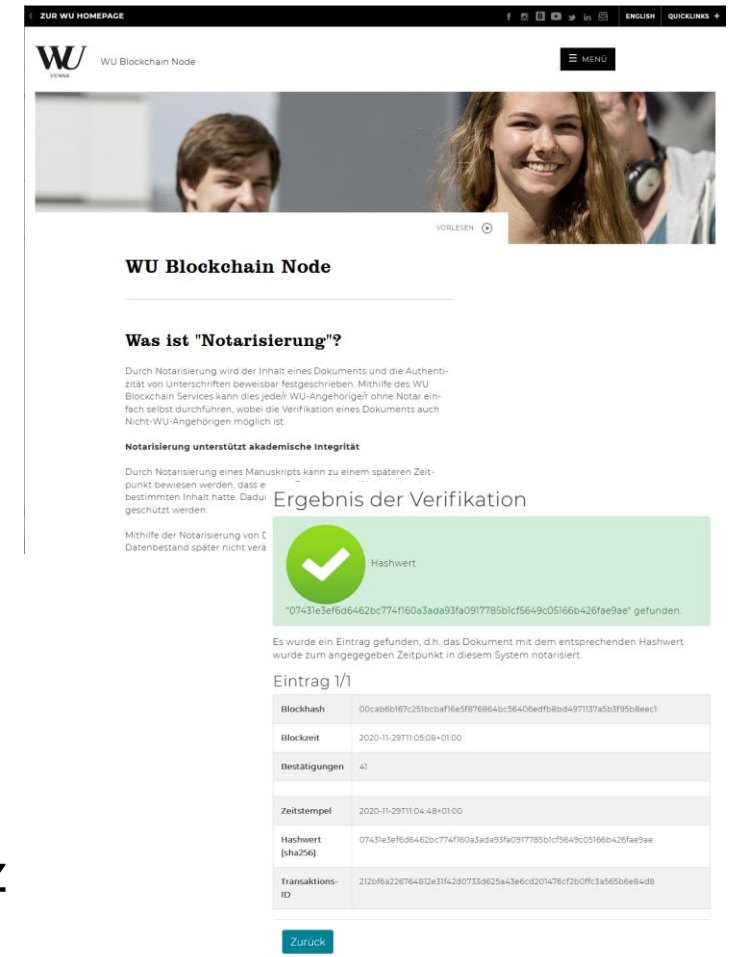
Austrian Public Service Blockchain („APSB“) - Status 6/2021

- (keine News)
- Initiative von Institutionen der öffentlichen Verwaltung
- „Konsortium-Blockchain“ für unterschiedliche Usecases im „public service“ Bereich
 - Blockchain in Echtbetrieb seit 10/2019
- Konsortialpartner derzeit
 - BRZ (Bundesrechenzentrum)
 - Stadt Wien
 - WKO (Wirtschaftskammer) - Daten-Zertifizierung
 - Nic.at (cert.at)
 - WU Wien - Blockchain-Node & Notarisierung
- 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 Österreich)	ja	ja
nic.at/cert.at	ja	ja
WU (Wirtschaftsuniversität Wien)	ja	ja
AUSTRIAPRO	(ja)	

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



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 and authenticity of a document. A green box displays the verification result: 'Ergebnis der Verifikation' with a green checkmark and the text 'Hashwert "07431e3ef6d6462bc774f160a3ada93fa091778501c5649c05166b426fae9ae" gefunden.' Below this, a table shows the entry details:

Eintrag 1/1	
Blockhash	00cab6b167c251bcbaf16e5f876864bc5640eefb8bc4971137a5b3f95bbaec1
Blockzeit	2020-11-29T11:05:08+01:00
Bestätigungen	41
Zeitstempel	2020-11-29T11:04:48+01:00
Hashwert (sha256)	07431e3ef6d6462bc774f160a3ada93fa091778501c5649c05166b426fae9ae
Transaktions-ID	2126f6a226764812e314290733d625a43e6cd201476cf2b0ff3a565b6e84-d8

A 'Zurück' button is visible at the bottom of the table.

APSB - WU (Wirtschaftsuniversität Wien)













- Neuer Usecase
 - 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

„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**

- „Blockchain Initiative Austria“
 - Offiziell gegründet 1/2021
 - <https://www.bc-init.at/>
 - Systembeschreibung & Rahmenbedingungen, Spezifikation Datenstruktur ...
 - Vereinsstatuten, Beitrittsantrag
- Aktuell (22.6.2021)
 - 13 Mitglieder & 1 Netzwerkpartner
 - Neu: Infinite Trust Digital GmbH
 - <https://infinite-trust-digital.com>

Aktuelle Mitgliederliste

AUSTRIAPRO - Verein zur Förderung standardkonformer E-Business Lösungen	
baumann.at - Blockchain Consulting & Development	
DEUDAT GmbH - Datenschutz und Informationssicherheit - Anwendung: Notarisierung	
IoT Austria - The Austrian Internet of Things Network	
IVM Technical Consultants GmbH	
RBKS - Dipl.-Ing. Roman Bruckberger-Koch	
SEC Consult Unternehmensberatung GmbH - Anwendung: ForensicForever	
Securikett Ulrich & Horn GmbH	
SIMTOOLS GmbH	
SYNERCON GmbH	
VIM Internetdienstleistungen GmbH	
Woschitz group GmbH	

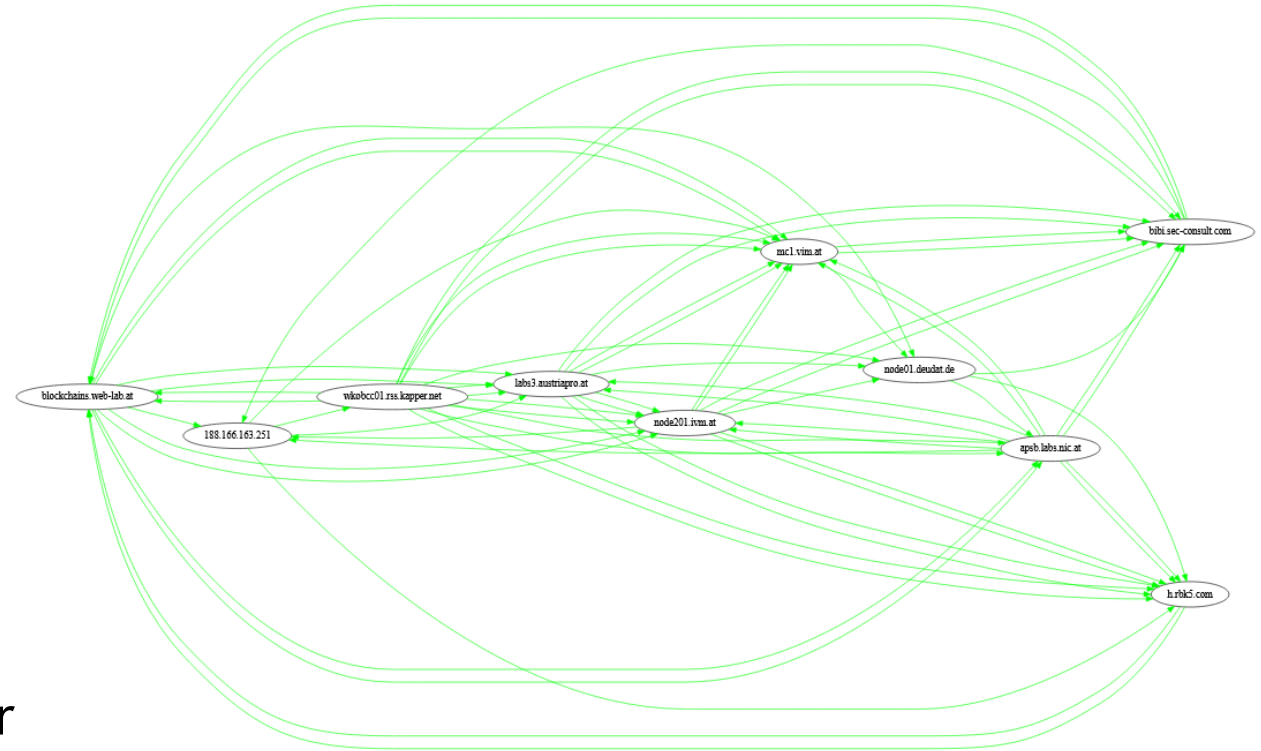
Ehrenmitglieder

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

Blockchain & Echtbetrieb

- Blockchain in Echtbetrieb seit 20.2.2020
 - Aktuell 11 Knoten
- Erster Use-Case: „Daten-Zertifizierung“
- 3 Anwendungen in Echtbetrieb
 - Dokumenten-Notarisierung „proof.li“
 - SEC Consult „ForensicForever“
 - DEUDAT.de - Notarisierung
 - (Demnächst) **Neu:** „Digitale Zertifizierung von Kosch & Partner RA GmbH“

datnos-20200220

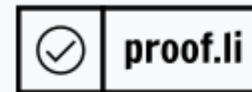


„proof.li“

- 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 ...



<https://proof.li/?voucher=38879111&auth=a8e2ee4512c568ce152925a018829>



Erstellen Verifizieren

OK, Gutschein gültig.

Gutschein '38879111' aktiviert.

Sie können nun Notarisierungen erstellen.

Gutschein-ID: 38879111, Transaktionsguthaben: **100**

News aus dem TestLab

- Projektbericht „Technische Erweiterungen für Konsortialblockchains auf Multichain-Basis“
- MultiChain Testnetz

DLT Development & Implementation

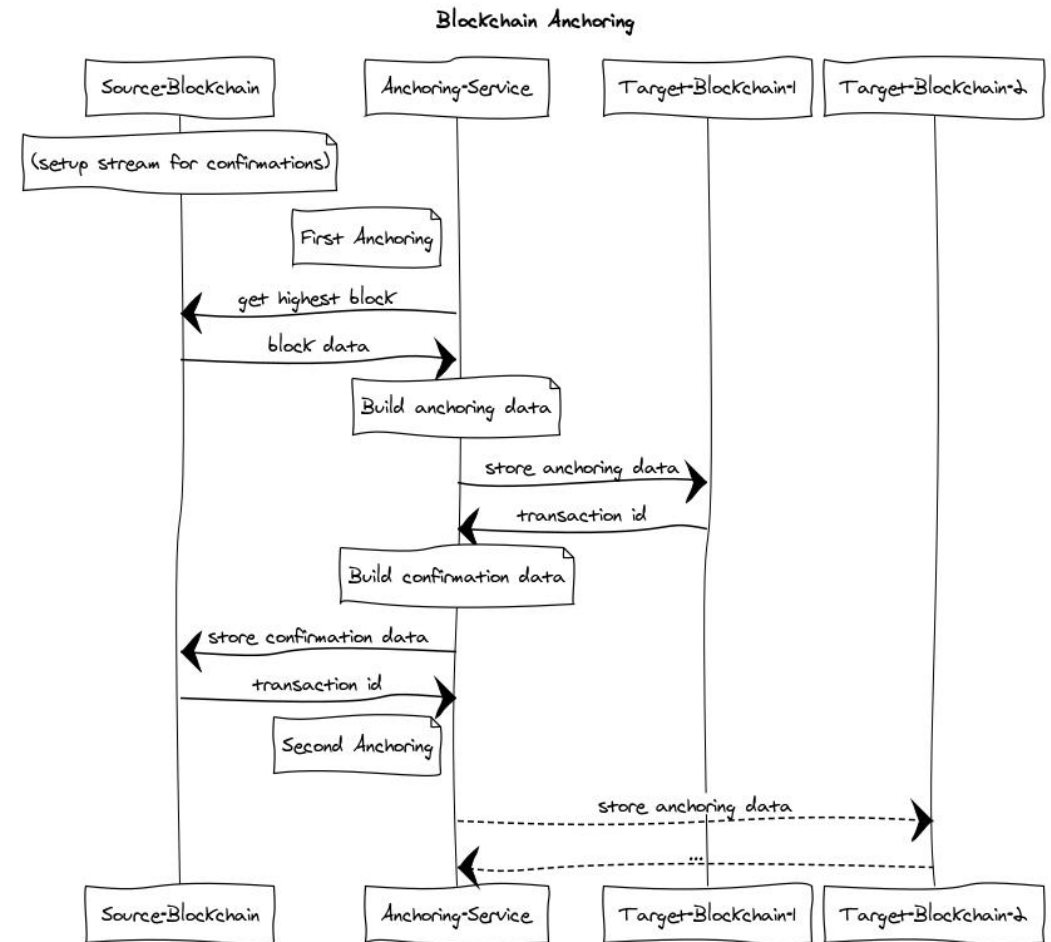
- Projekt von ABC-Research
 - unterstützt von AustriaPro
 - Subprojekt: „Technische Erweiterungen für Konsortialblockchains auf Multichain-Basis“
- Themen im Zusammenhang mit
 - Austrian Public Service Blockchain
 - Private Sector Blockchain
- Themen
 - Anchoring
 - Member Management (Integrierte Teilnehmerverwaltung)
 - Automatisierung (Mail-Notarizer, File-Notarizer)
 - Erweiterte Verifikation („Verify+“)

Anchoring

- Notarisieren des aktuellen Zustandes einer Blockchain in einer anderen Blockchain
 - Typischerweise um eine „kleine“ Blockchain ...
 - ... in eine „große“ zu verankern
 - Z.B. private oder Konsortiumchain mit wenigen Nodes in eine public Blockchain
- Zweck: Nachweis dass die Source-Chain
 - nicht manipuliert wurde
 - bzw. potentielle Manipulationen erkannt würden
- Daten des jeweils aktuellen Blocks
 - Blocknummer
 - Block-Hash
 - Zeitstempel

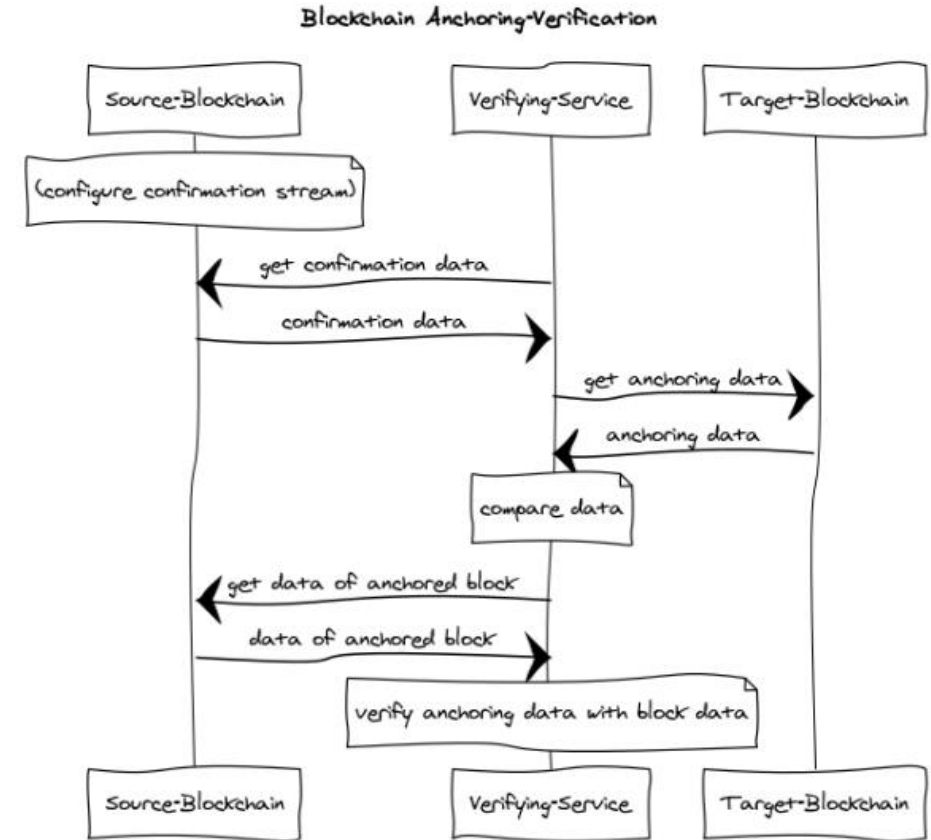
Anchoring - Ablauf

- Aktuelle Blockdaten von Source-Chain abfragen
- Daten aufbereiten (Json ...)
- Transaktion in Target-Chain durchführen
- Ergebnis (Bestätigung) in Source-Chain protokollieren



Anchoring - Ablauf Verifikation

- Bestätigung aus Source-Chain lesen
- Anchoring data in Target-Chain suchen
- Daten vergleichen
- Blockdaten in Source-Chain verifizieren



Anchoring - Details

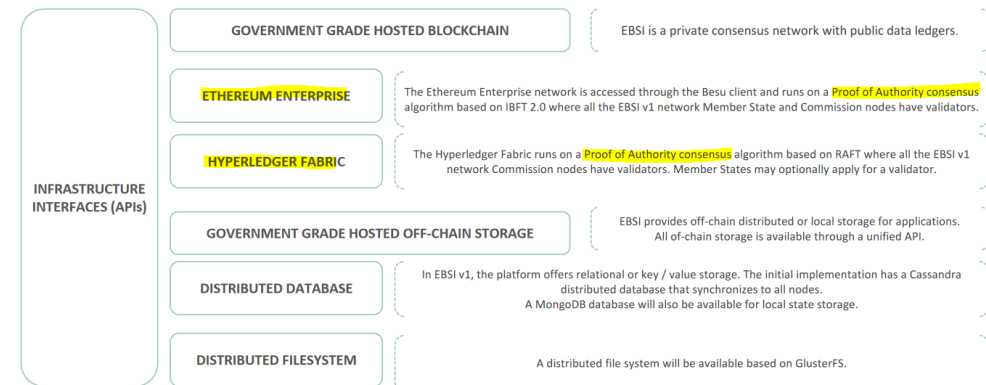
- Unterschiedliche Target Chains
 - „Größe“, Kosten ...
- Weitere Aspekte
 - Datenstrukturen
 - Konfigurationen
 - Beispiele incl. Code
 - Konnex zu EBSI?
 - European Blockchain Services Infrastructure

Blockchain	Anzahl aktiven Nodes an (Full-)	Kosten pro Transaktion (grober Bereich)	Größenbeschränkung pro Transaktion
Bitcoin	Ca. 9000 ¹⁷	€ 0,50 – 5,00	80 Bytes
Ethereum	Ca. 4000 ¹⁸	€ 1,00 - 10,00	Keine (für diesen Usecase relevante)
Waves	Ca. 300-500 ¹⁹	€ 0,02 – 0,05	Keine (Kosten: 0,001 WAVES pro kB)

EBSI native blockchain and storage APIs

Integrate any application to the EBSI infrastructure using the Infrastructure APIs

As an alternative to using the Core Services APIs, applications may be integrated to native APIs where developers choose to create additional functionality to the ones available.



Member Management

- Organisatorische und technische Verwaltung der Mitglieder einer Konsortium Chain
- Off-chain
 - ...
- On-chain
 - Speicherung von ausgewählten Daten in der Blockchain selbst
 - Bereitstellung durch die Blockchain
 - Automatische Auflösung von Blockchain-Adresse zu (menschenslesbaren) Bezeichnungen
 - „Wer hat eine Transaktion signiert“
 - z.B. einen Eintrag in einen Blockchain-Stream

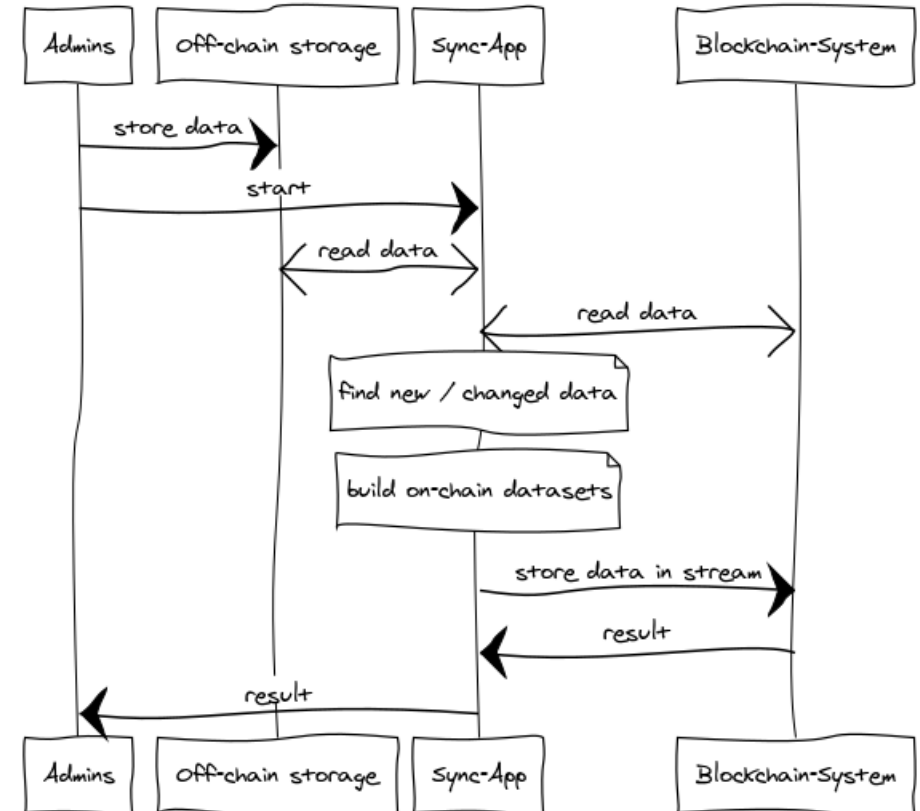
Member Management - Synchronisierung

- Synchronisierung
 - Off-chain daten
 - Teile für on-chain geeignet

Beispiel in JSON:

```
{  
  "address": "1KzUbXU7QGm8ecNSeBGgCQKX8JYzNZjYxgmoFq",  
  "label": "node#blockchains.web-lab.at",  
  "owner": "baumann.at",  
  "isNode": true,  
  "location": "Europe\\Frankfurt",  
  "remarks": "Hetzner",  
  "active": true,  
  "version": "0.2"  
}
```

Member Management - Syncs with Blockchain



Member Management - Nutzung

- Blockchain / Applikationen
 - „interne Listen“
 - z.B. Permissions ...

- Publikation
 - „Mitglieder-Register“ von Konsortiumchains, automatisch aus Blockchain generiert

 - Veröffentlichung auf firmeneigener Webseite
 - Z.B. Impressum

Current Permissions

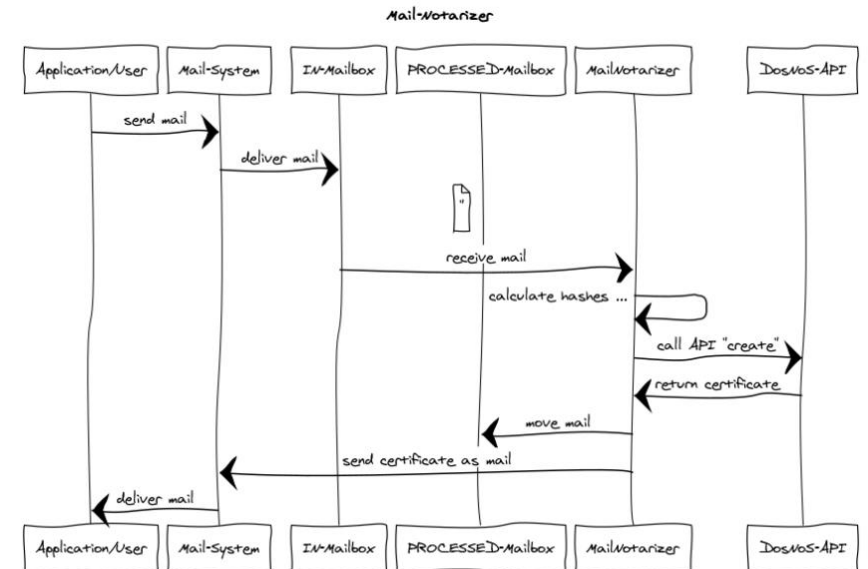
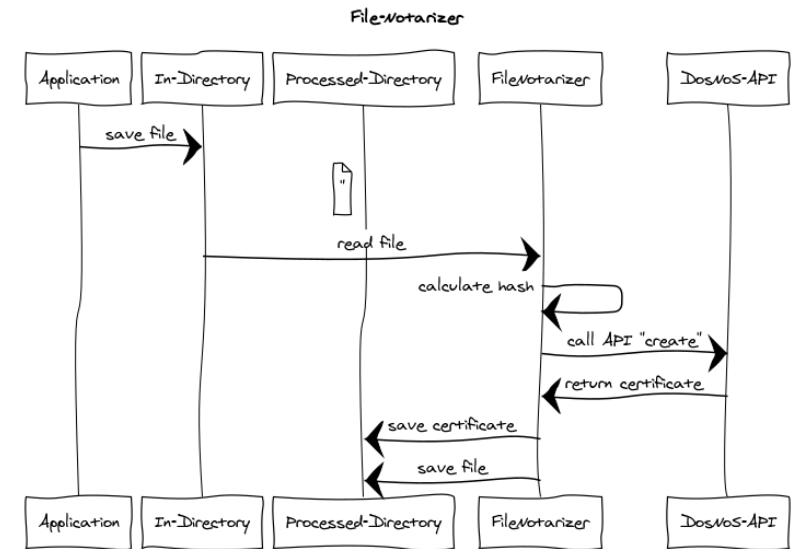
Label3	syn#test.baumann.at
Address	1JQhLuexFQjDAwxtnRAnV1m3jkNbakNsJNLJnz (local)
Permissions	mine, admin, activate, connect, send, receive, issue, create
Label	Fullnode@FRA
Label3	node#blockchains.web-lab.at
Address	1KzUbXU7QGm8ecNSeBGgCQKX8JYzNZjYxgmoFq
Permissions	mine, admin, activate, connect, send, receive, issue, create
Label	rbk@aws1-MC2a3
Label3	node#aws.rbk5.com
Address	1Z1XVEh5CTEiEmr165b6mhg8MuwXpotTm9vXX2
Permissions	connect, send, receive, issue, create

Adresse	Owner	Label
1CH6vFo3UM...Rqmh8Dtz5L	ABC Research GmbH	node#abc-research.at
1JQhLuexFQ...akNsJNLJnz	AustriaPro (WKO)	members#austriapro.at
1Z1XVEh5CT...potTm9vXX2	Blockchain Initiative Austria	docnos#proof.li
...		

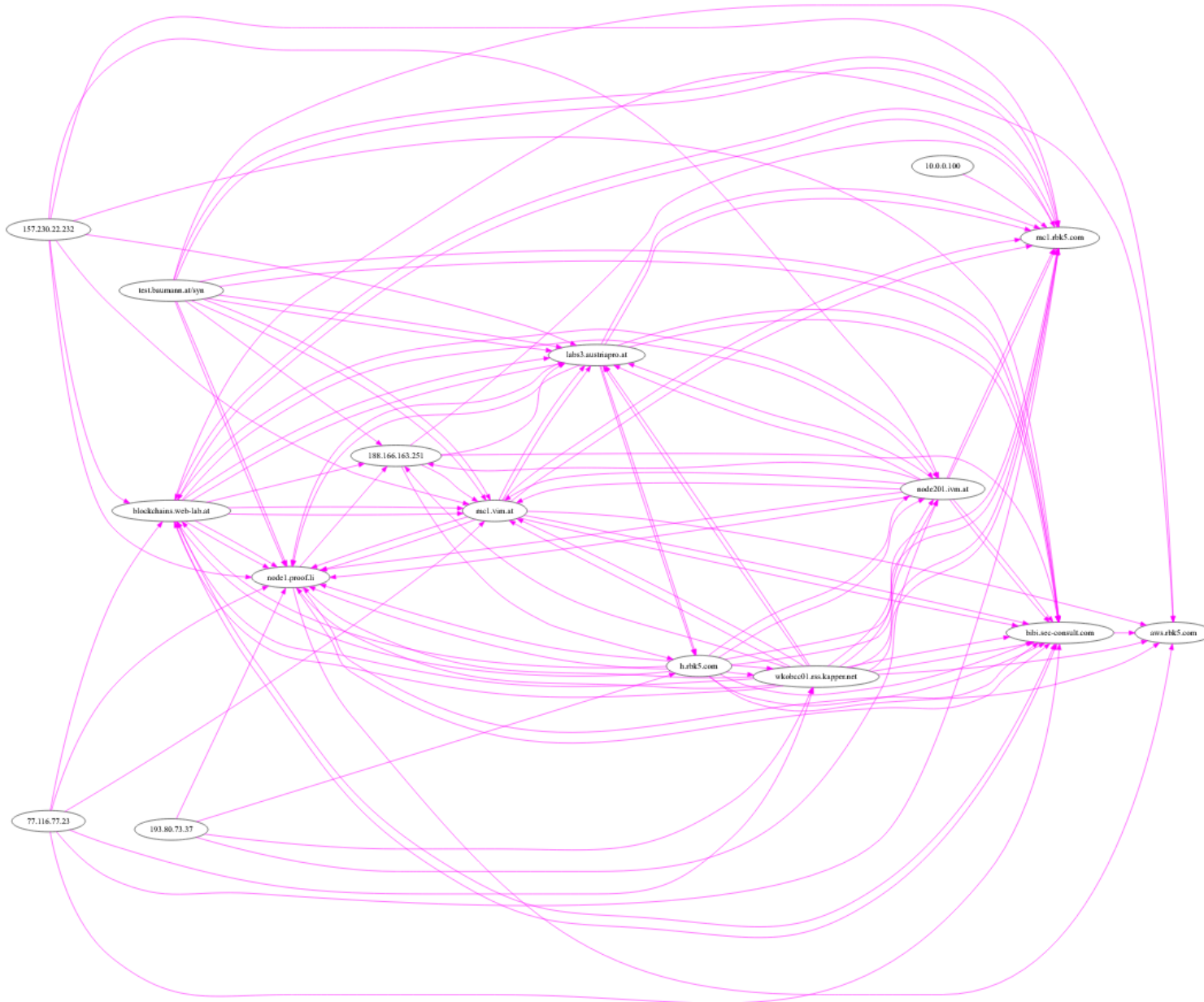
Automatisierung

- File-Notarizer
 - Automatische Verarbeitung von Files (Serververzeichnisse ...)
 - Integration in andere automatisierte Prozesse
 - ...

- Mail-Notarizer
 - = E-Mail-Client
 - Automatische Verarbeitung von Mails / Attachments
 - Integration in mailbasierte Workflows
 - ...



mc2b1



Multichain Test-Netz

- AustriaPro Lab
- & friends
- Diverse Beispiele (Code) verfügbar (github)
- Offen für weitere Teilnehmer
- **MITMACHEN!!!**

- Vorschau Blockchain Award 2021
- Kooperation mit DIO (Data Intelligence Offensive)
- open space - Projekte, Initiativen, Informationen

open space - Projekte, Initiativen, Informationen

- Rocklogic: David Scheidl
- DLT Austria: Eduard Prinz

- 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

