DocNoS/DatNoS

Document & Data Notarization
Verfügbare Services & Module
12/2024 (v5)

AUSTRIA PRO

Übersicht

- Usecase DocNoS
  - Austrian Public Service Blockchain
  - Private Sector Blockchain
- Usecase DatNoS
- Software-Module verfügbar
  - Quellen: AustriaPro-Lab, BC-Initiative, 3rd party
  - Produktion (Test, Prototyp)

- Links siehe
  - AustriaPro Lab Links-Seite
  - BC-Init Webseite

AustriaPro Blockchain Lab

Diese Seite beinhaltet Links zu diversen Themen und Ergebnissen des Arbeitskreises Blockchain der AustriaPro und dem "Blockchain-Lab". Weiters werden Informationen von inhaltlich verwandten Systemen bzw. Organisationen aufgelistet.
Bitte beachten: Da es sich um ein "Lab" handelt, in dem oft experimentiert wird, kann es vorkommen, dass nicht immer alle Services verfügbar sind bzw. korrekt funktionieren.

Dokumentation

- AustriaPro Arbeitskreis Blockchain: Kurzbeschreibung, Termine, Protokolle und Präsentationen (2018 - 2023) sowie weitere Links.

Demos Blockchain und Keys (laufen im Webbrowser)

- Blockchain Demo - By Anders Brownworth - Erweiterung Strukturierte Daten - Erweiterung Strukturierte Daten - Beispiele Daten-Zertifizierung
- Public/Private Keys & Signing - By Anders Brownworth

MultiChain

Die Opensource Blockchain Umgebung MultiChain ist das im Lab am meisten verwendete System.

Tools, Anleitungen

- Multichain Node im AustriaPro Lab auf Basis Docker installieren - Anleitung für Lab-Node "apro-lab-2" (2023)
- Multichain API Library (PHP) (2022)
- Demos for AustriaPro Blockchain Lab - Schreiben und Lesen in/von Multichain Streams (Sourcecode in PHP). (2022)

Node AustriaPro Lab 1 (-> 2022)

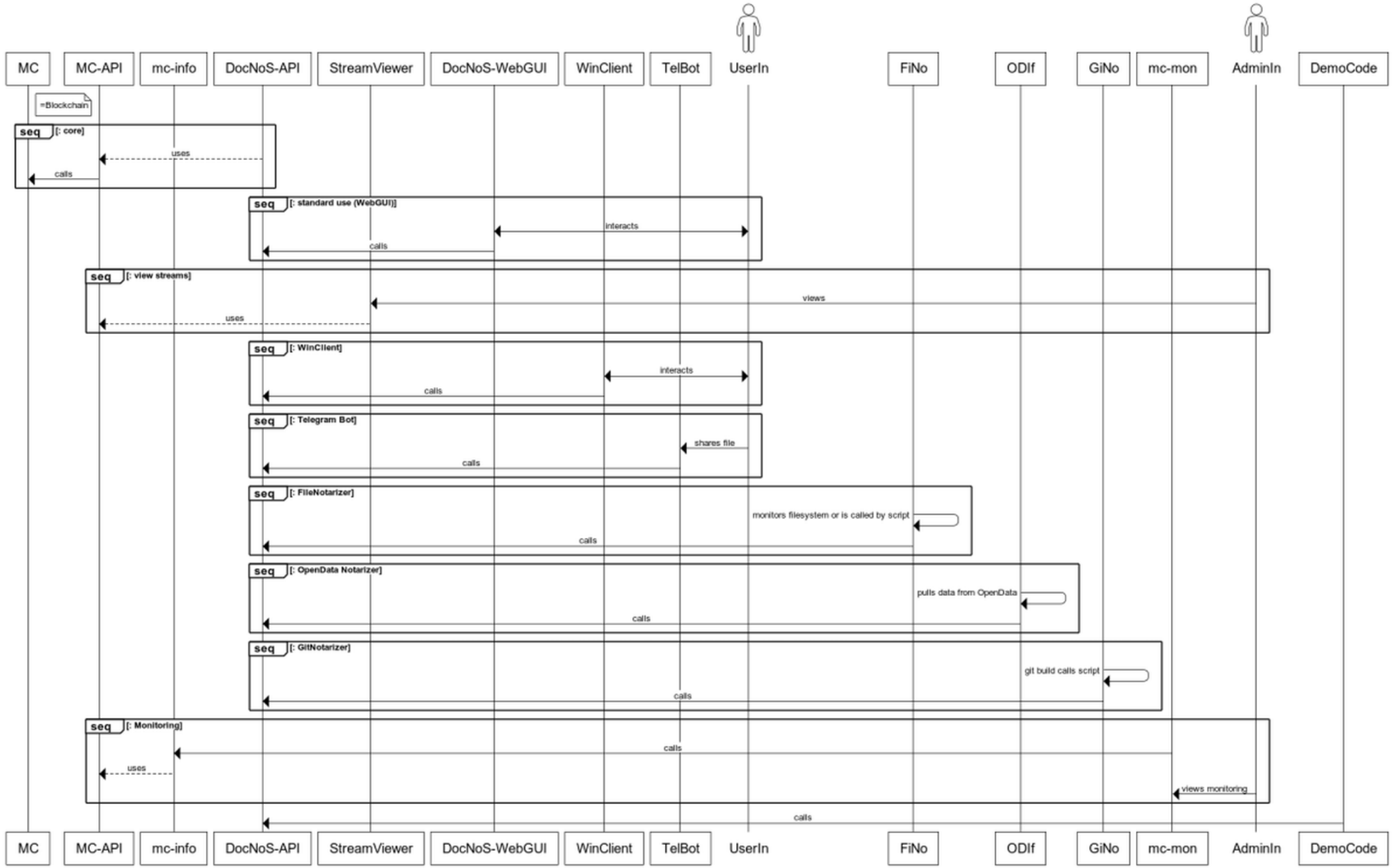
- Web-GUI für einen der im Lab installierten Blockchain-Nodes
- Proof Of Existence - Demo

Node AustriaPro Lab 2 (ab 2023)

DocNoS/DatNoS?

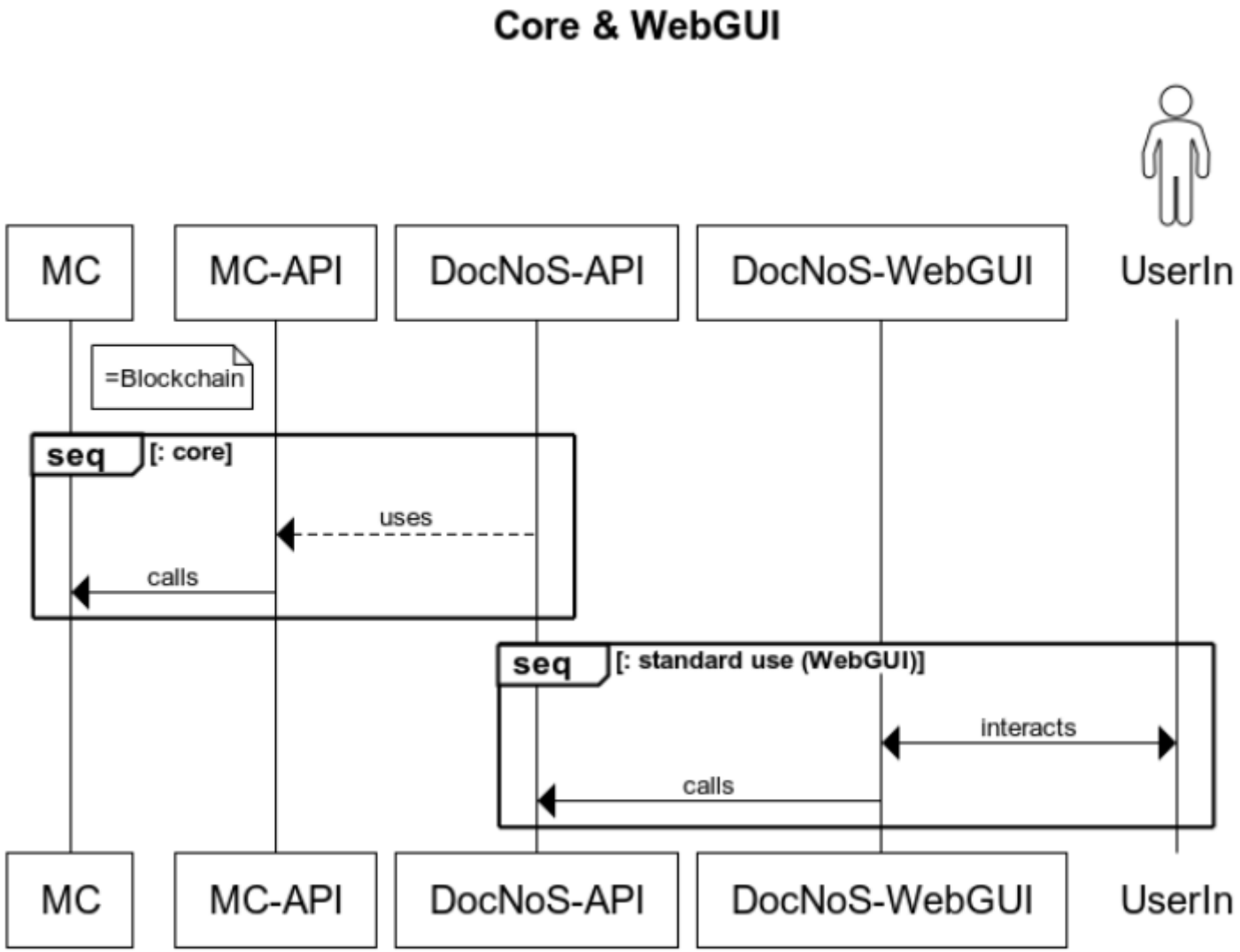
- DocNoS – Document Notarization Service
  - Speicherung von Hashwerten in der Blockchain
  - Daten sind/bleiben in der Usersphäre
  - Beispiele
    - Austrian Public Service Blockchain (WKO, WU, BMSGPK …)
    - Private Sector Blockchain (Mitglieder Blockchain Intitiative Austria)
- DatNoS – Data Notarization Service
  - Speicherung von Daten in der Blockchain
  - Unverschlüsselt (öffentlich sichtbar) oder verschlüsselt
  - Beispiele
    - Öffentlich verfügbare Daten (zB auf data.gv.at)
    - Zu veröffentlichende Daten
    - Achtung: keine personenbezogenen Daten
  - Mehrere Testchains: Mitglieder Blockchain Intitiative Austria

DocNoS Landscape & Artifacts

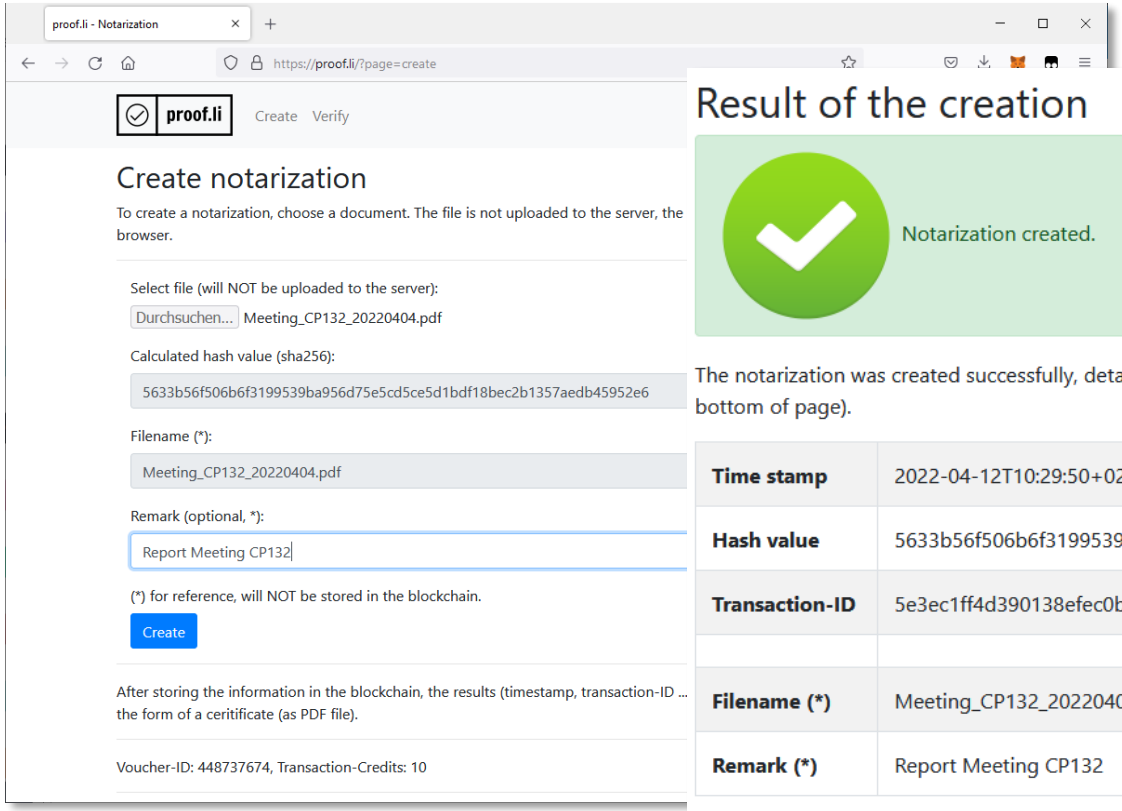


Core & WebGUI

- 2 produktive Chains (APSB, PSBC), mehrere Test-Chains
- MC-API
  - OS, Github
  - Beispiel-Code
- DocNoS-API
  - Specification
  - Beispiel-Code
- Web-GUI
  - Einsatz auf vielen Systemen
  - Create/Verify (Dual)

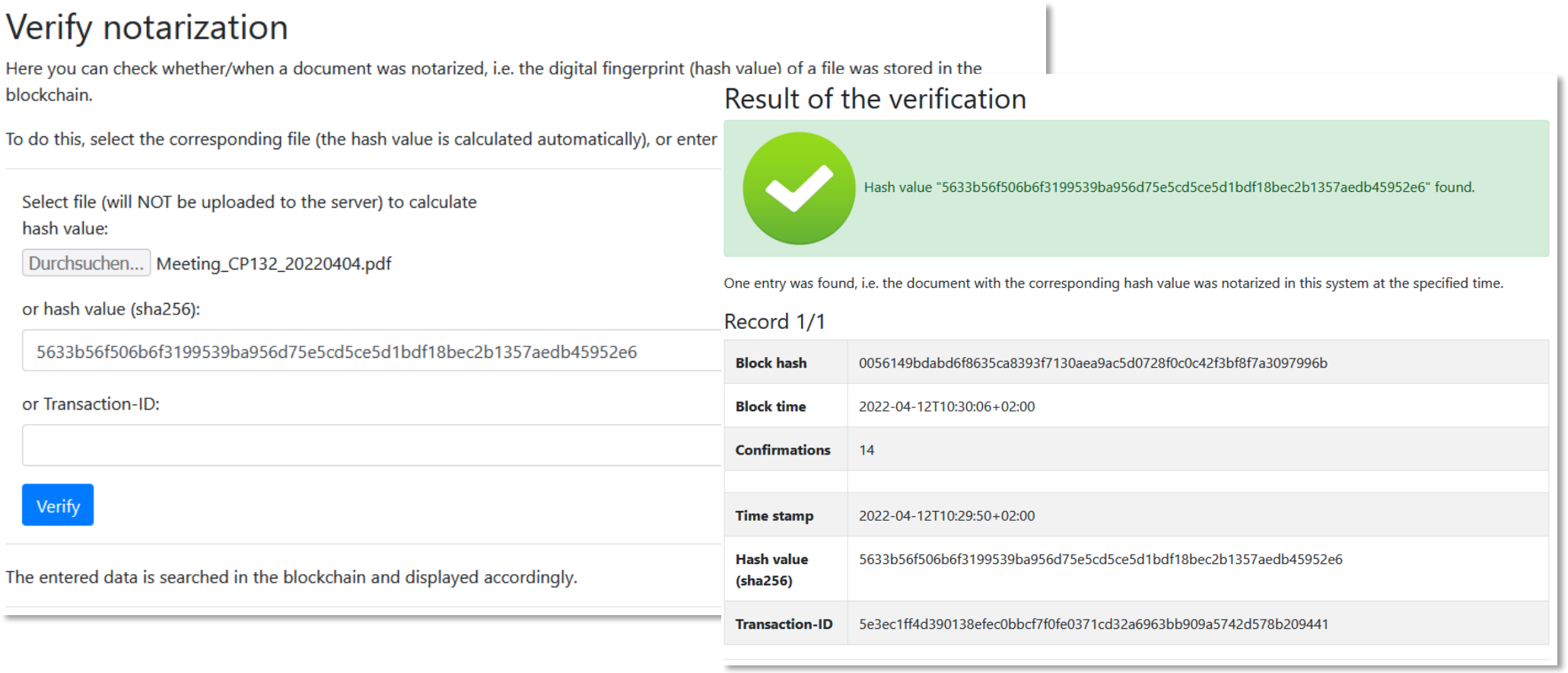


Notarization – Creation (Beispiel: Web-GUI)



Example „proof.li“ operated by https://bc-init.at

Notarization – Verification (Beispiel: Web-GUI)

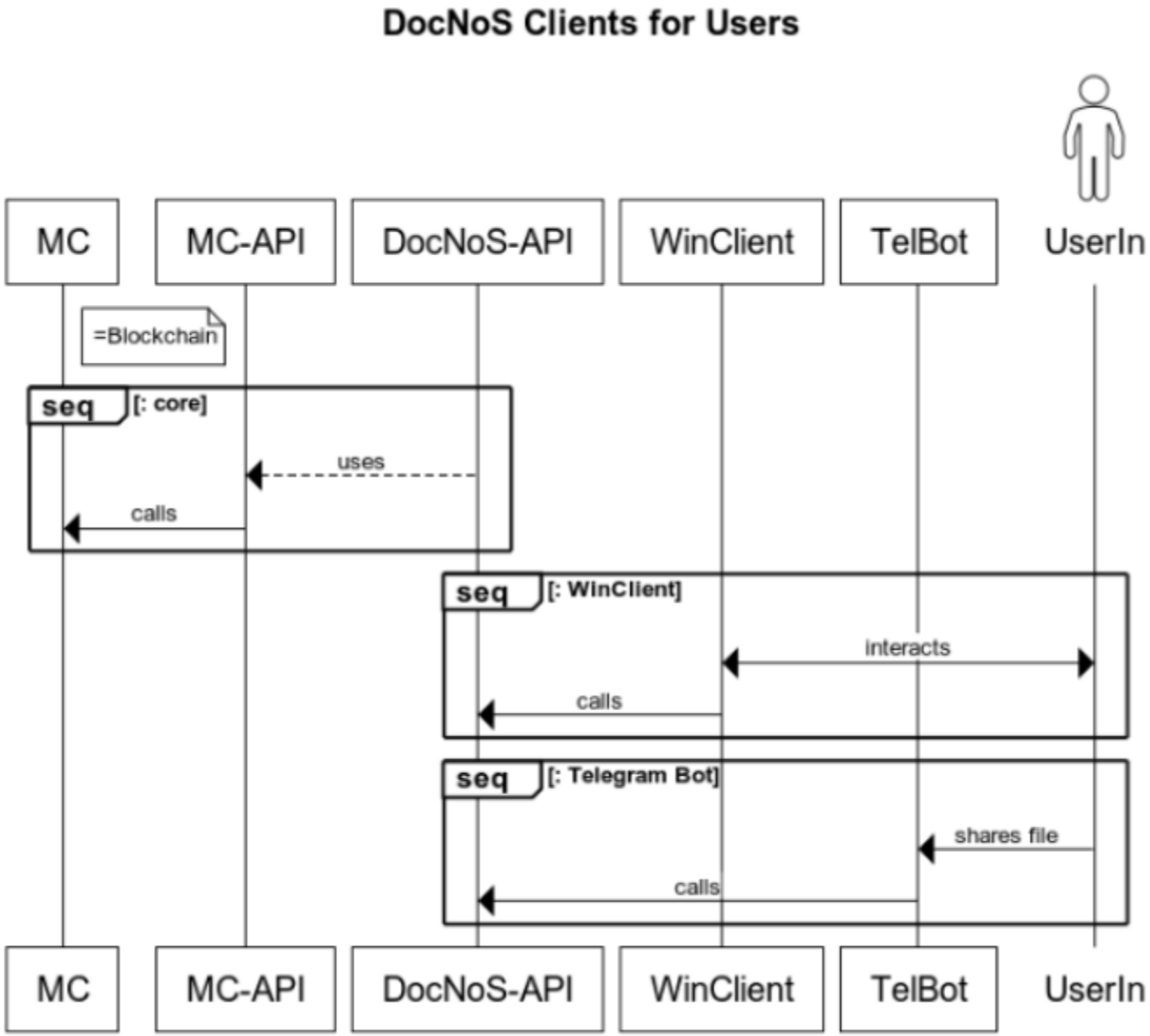


AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

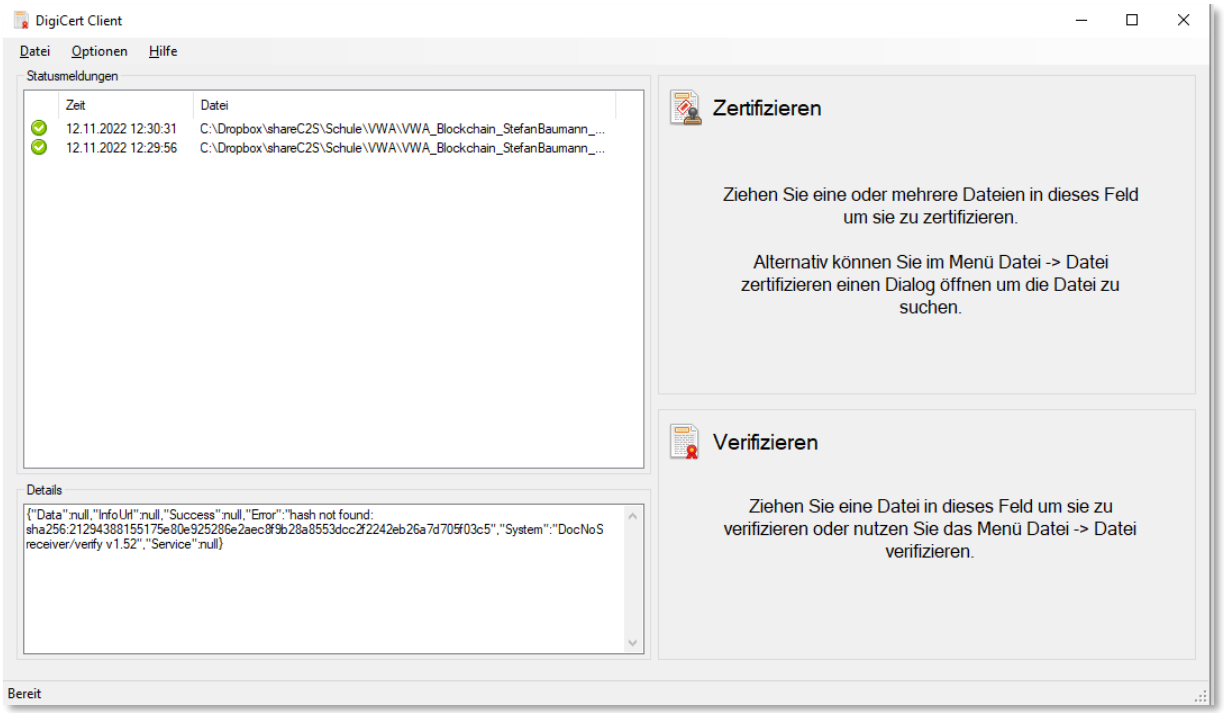
Clients für User

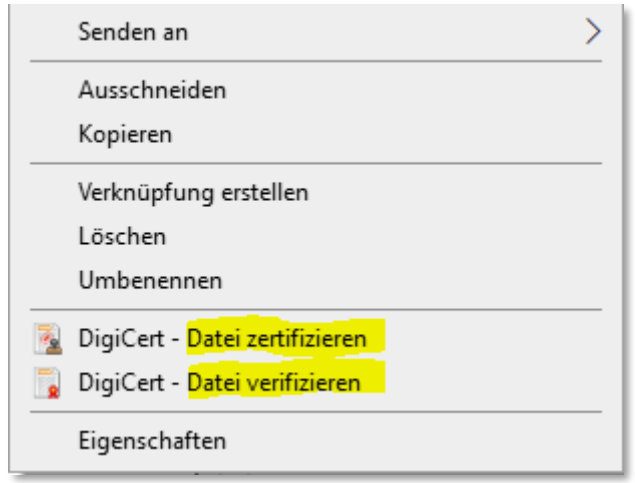
- Windows-Client
  - 3rd party
  - PSBC: mehrere Anwendungen
  - APSB: WU
- Telegram Bot
  - Prototyp auf Test-Chain



DigiCert Client

- Windows Desktop Programm
- Nutzung via Menü, drag & drop oder Kontextmenü



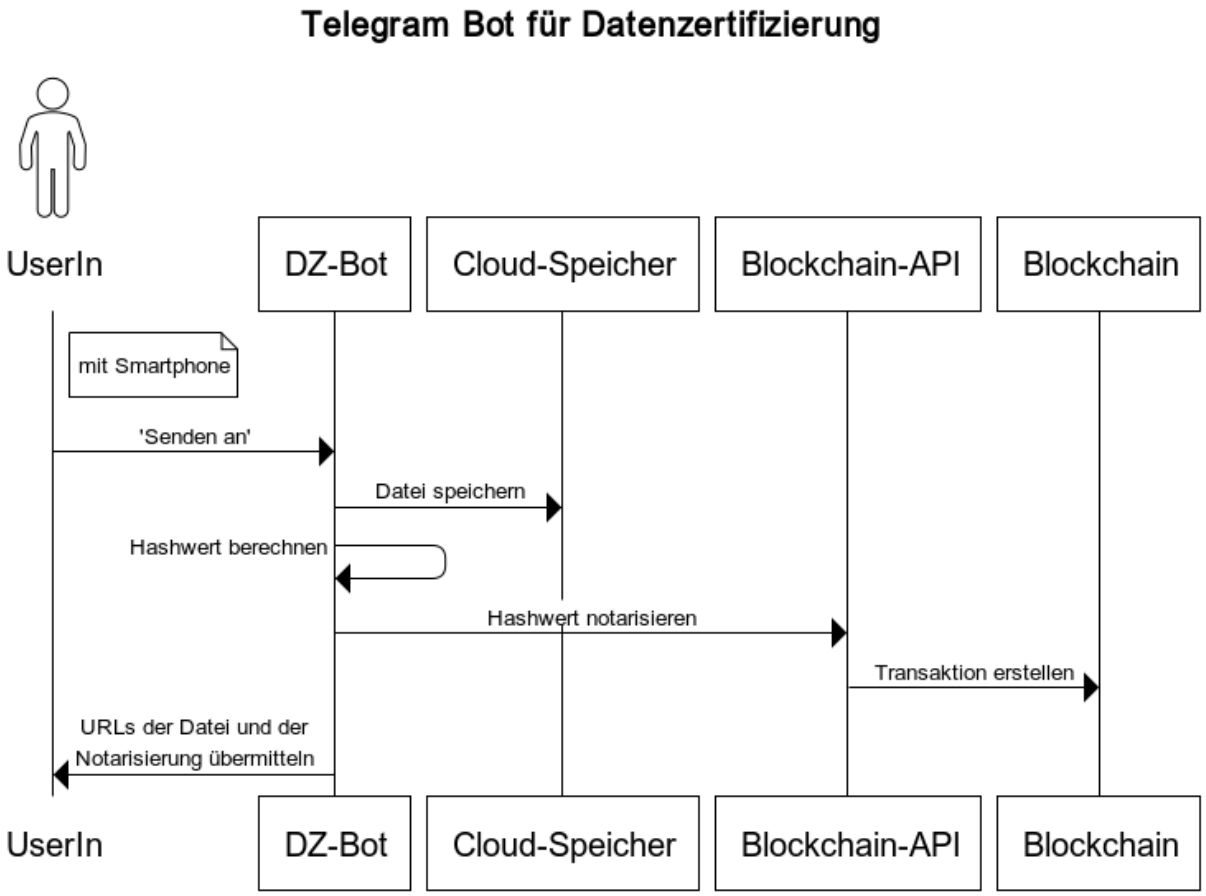


AUSTRIA PRO

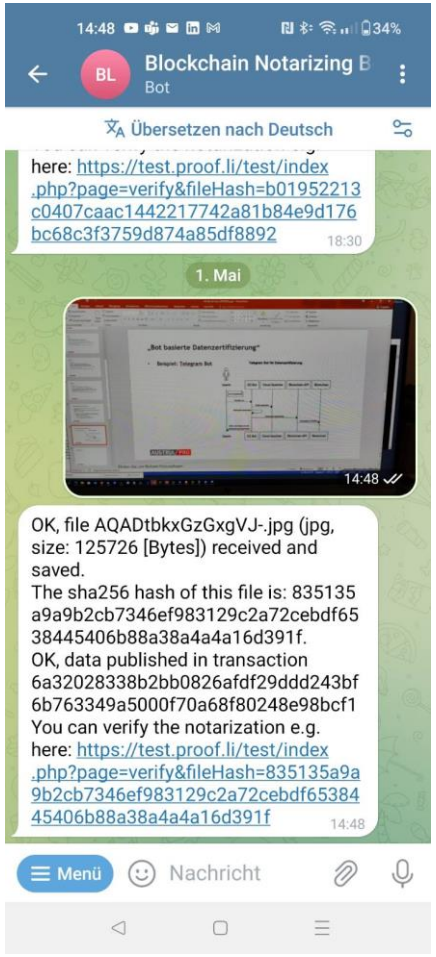
BLOCKCHAIN INITIATIVE AUSTRIA

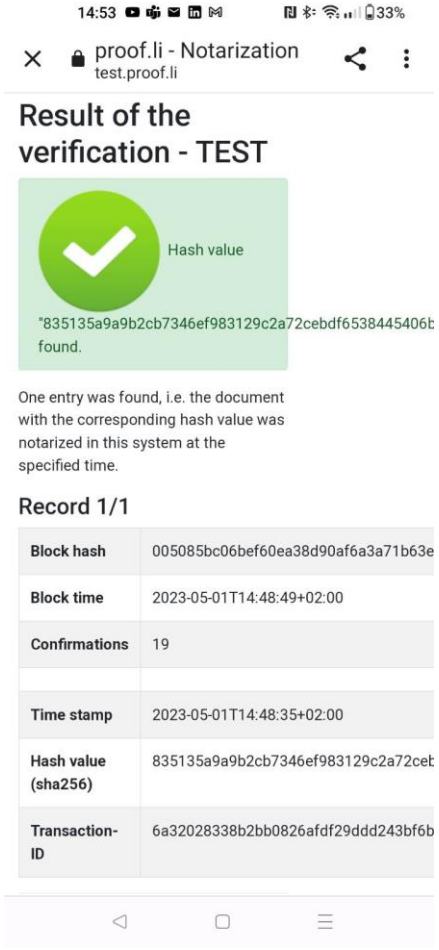
„Bot basierte Datenzertifizierung“

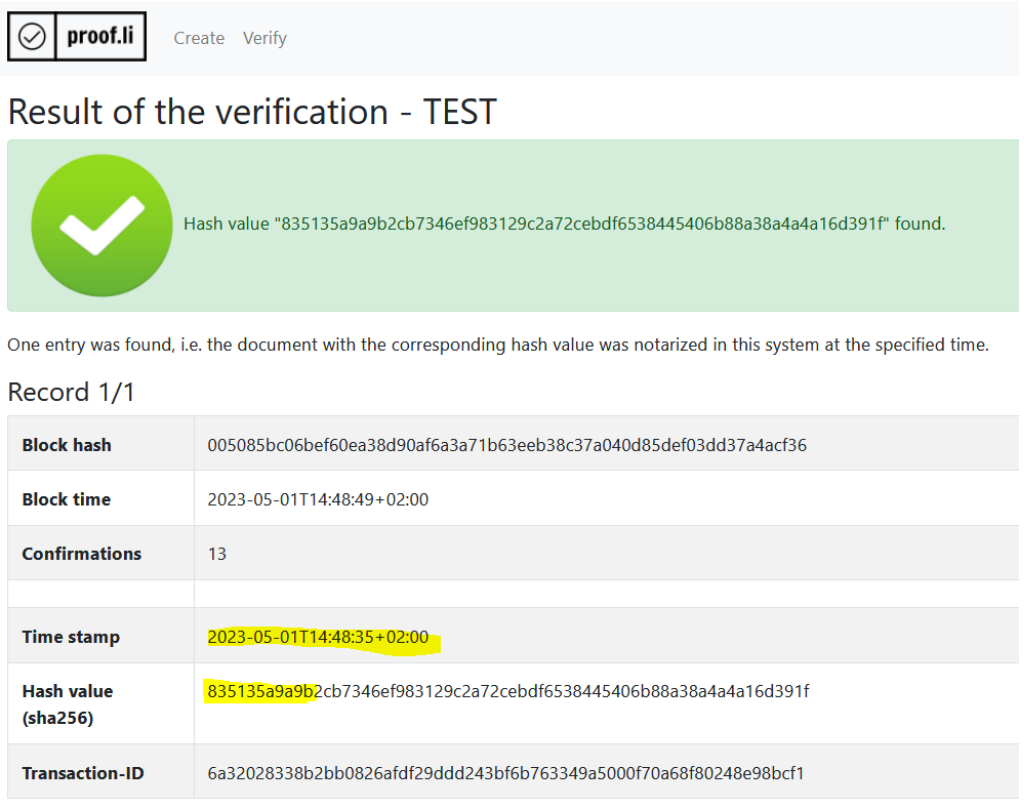
- Beispiel: Telegram Bot
  - „Senden an“
  - (Speichern)
  - Hashwert errechnen und notarisieren
  - Ergebnis an User
- @BlockchainNotarizing_bot



Telegram Bot: „Blockchain Notarizing Bot“





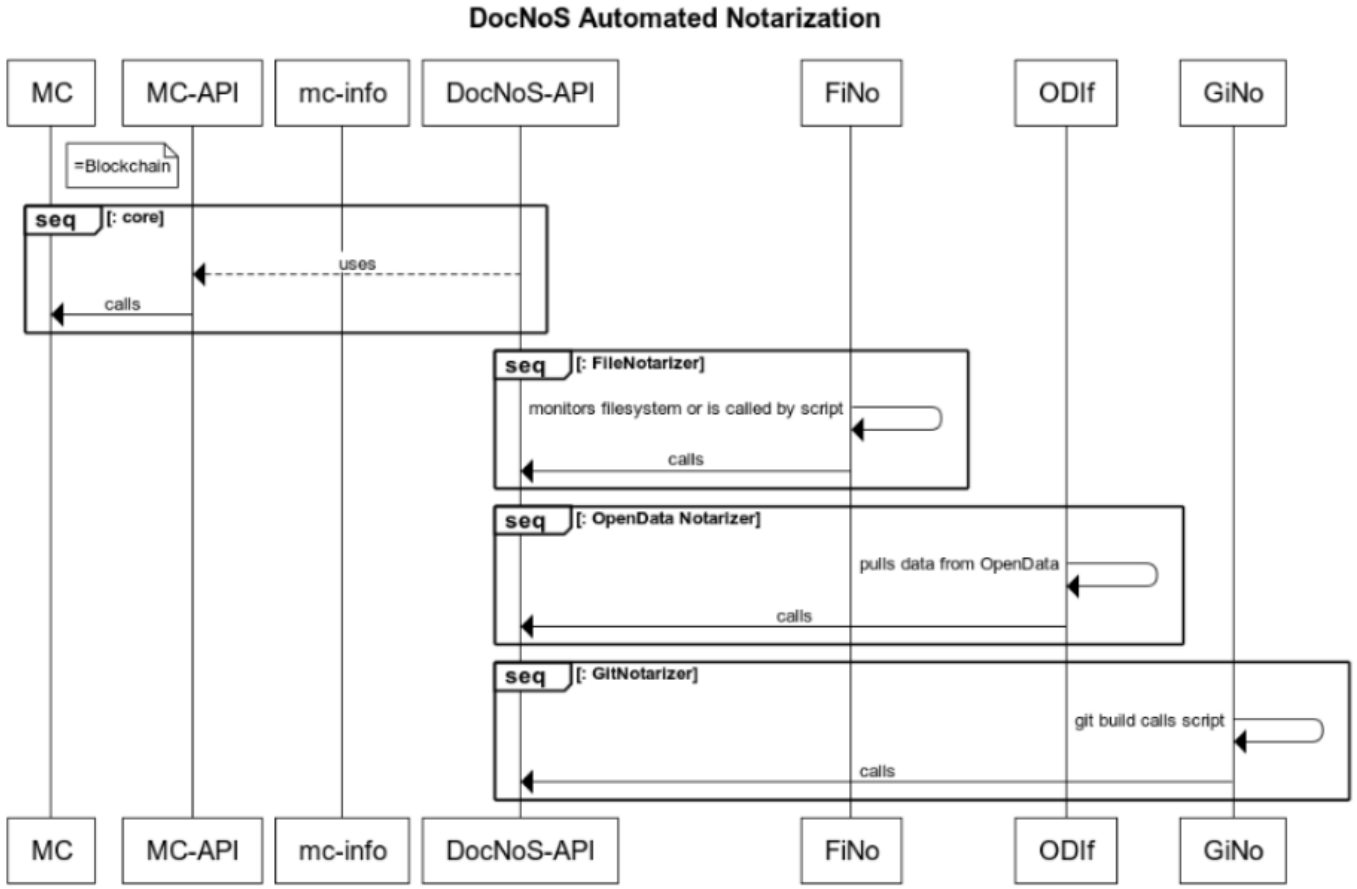


AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

Automatisierte Notarisierung

- File-Notarizer
  - ZB. BMSGPK
- OpenData Interface
  - Air Quality Chain
  - Wien OGD-Metadaten (in Entwicklung)
- Git-Notarizer
  - SW-Artetakte
  - In Build-Pipeline



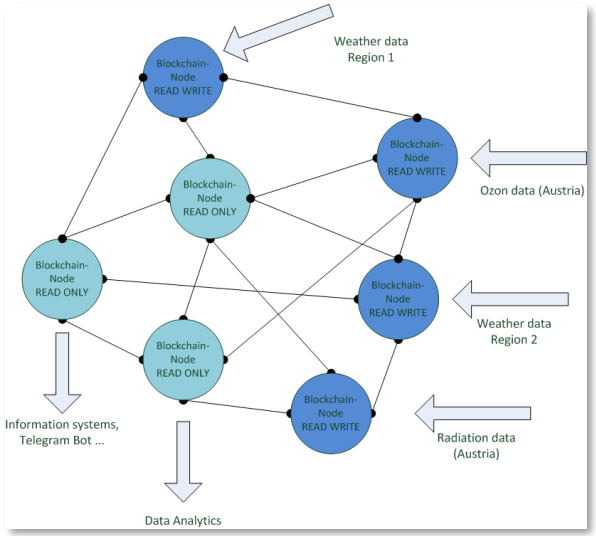
Beispiel AQC (Air Quality Chain)

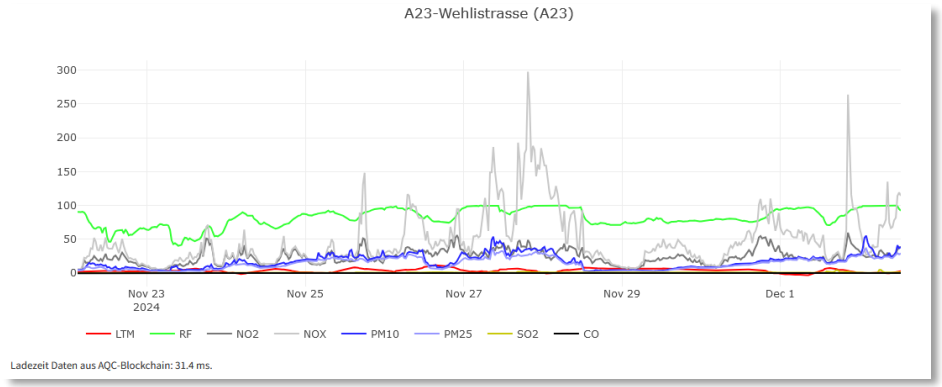
Stream: aqc-messdaten – 1000 of 7530 items with key: KEND

Publishers	MC2.0a@FRA (1AW7CVnQwpKPvxM7Hun3EYzfZKDZPfDNdpHSE3)
Key	KEND
Data	{"station":"KEND","zeit":"2018-09-03T11:00:00+02:00","werte":{"WG":1.73,"WR":140.23,"NO2":28.91,"NOX":34.3,"PM10":12.88,"PM25":10.45}}
Added	2018-09-03 09:15:02 GMT

Publishers	MC2.0a@FRA (1AW7CVnQwpKPvxM7Hun3EYzfZKDZPfDNdpHSE3)
Key	KEND
Data	{"station":"KEND","zeit":"2018-09-03T10:30:00+02:00","werte":{"WG":3.43,"WR":105.15,"NO2":26.74,"NOX":32.69,"PM10":12.33,"PM25":10.51}}
Added	2018-09-03 08:45:01 GMT

Publishers	MC2.0a@FRA (1AW7CVnQwpKPvxM7Hun3EYzfZKDZPfDNdpHSE3)
Key	KEND
Data	{"station":"KEND","zeit":"2018-09-03T10:00:00+02:00","werte":{"WG":2.61,"WR":124.64,"NO2":37.42,"NOX":46.46,"PM10":15.37,"PM25":12.47}}
Added	2018-09-03 08:15:02 GMT





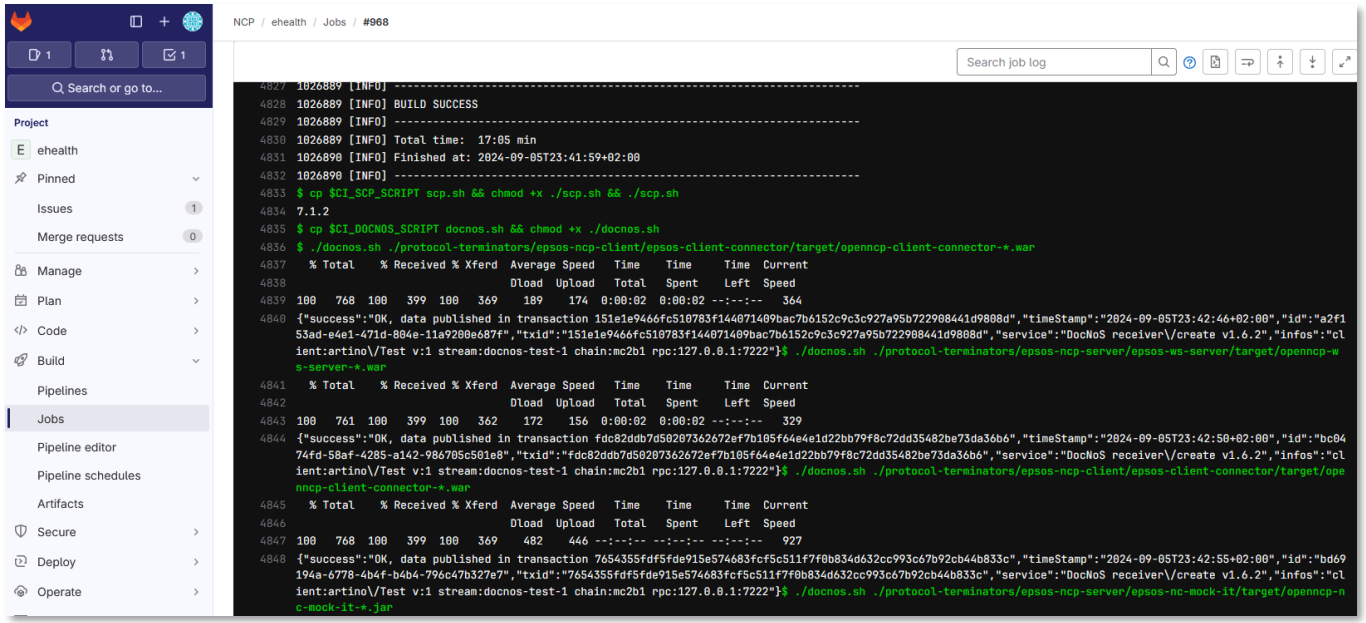
Details siehe Präsentation Roman Bruckberger-Koch

AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

Beispiel Git-Notarizer - Einsatz

- Beweis, wann welches SW-Artefakt gebaut wurde
- Notarisierung der Hashwerte
  - Git-Commit-ID
  - Artifacts (.jar, .war)
- Integration in Build-Prozess
  - vollautomatisch
- Einsatz zB. im BMSGPK
  - Java Entwicklung
  - Lokales GitLab Repository
  - Usecase „OpenNCP“

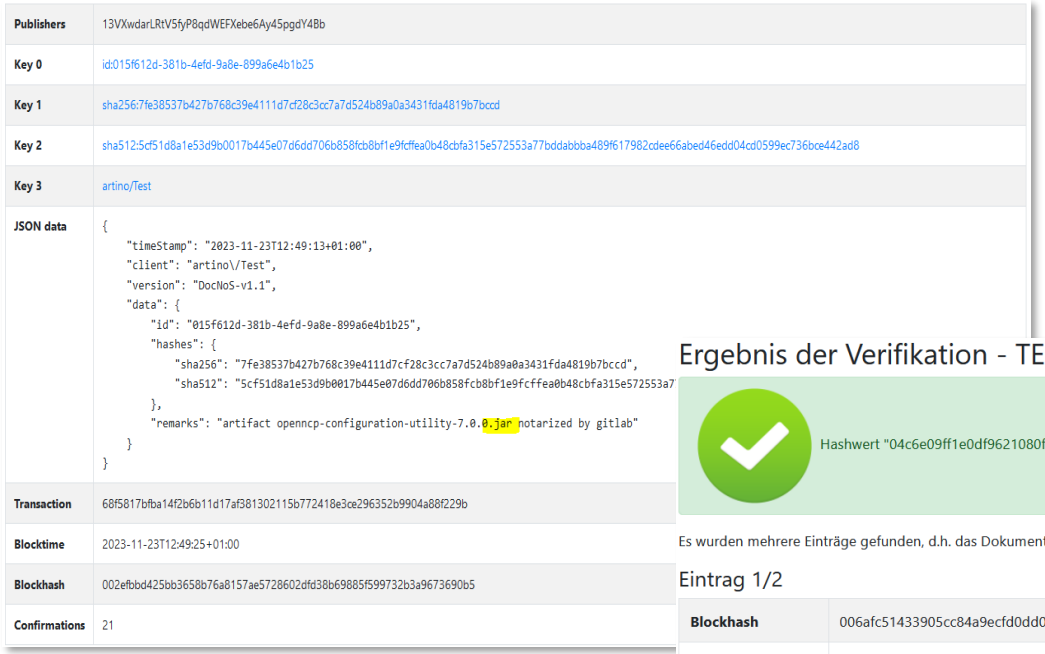


AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

Beispiel Git-Notarizer - Verifizierung

- Verifizierung per Blockchain
- Stream-Viewer
- oder Web-GUI



Publishers	13VXwdarLRtV5fyP8qdWEFXebe6Ay45pgdY4Bb
Key 0	id:015f612d-381b-4efd-9a8e-899a6e4b1b25
Key 1	sha256:7fe38537b427b768c39e4111d7cf28c3cc7a7d524b89a0a3431fda4819b7bccd
Key 2	sha512:5cf51d8a1e53d9b0017b445e07d6dd706b858fcb8bf1e9fcffea0b48cbfa315e572553a77bddabbba489f617982cdee66abed46edd04cd0599ec736bce442ad8
Key 3	artino/Test
JSON data	{ "timeStamp": "2023-11-23T12:49:13+01:00", "client": "artino\/Test", "version": "DocNoS-v1.1", "data": { "id": "015f612d-381b-4efd-9a8e-899a6e4b1b25", "hashes": { "sha256": "7fe38537b427b768c39e4111d7cf28c3cc7a7d524b89a0a3431fda4819b7bccd", "sha512": "5cf51d8a1e53d9b0017b445e07d6dd706b858fcb8bf1e9fcffea0b48cbfa315e572553a7 }, "remarks": "artifact openncp-configuration-utility-7.0.0.jar notarized by gitlab" } }
Transaction	68f5817bfba14f2b6b11d17af381302115b772418e3ce296352b9904a88f229b
Blocktime	2023-11-23T12:49:25+01:00
Blockhash	002efbbd425bb3658b76a8157ae5728602dfd38b69885f599732b3a9673690b5
Confirmations	21

Ergebnis der Verifikation - TEST

Hashwert "04c6e09ff1e0df9621080ffb3c534fbb96fc07ef5db9533d5777f8d714bc03f1" gefunden.

Es wurden mehrere Einträge gefunden, d.h. das Dokument wurde mehrfach notarisiert. Der älteste Eintrag (der erste in

Eintrag 1/2

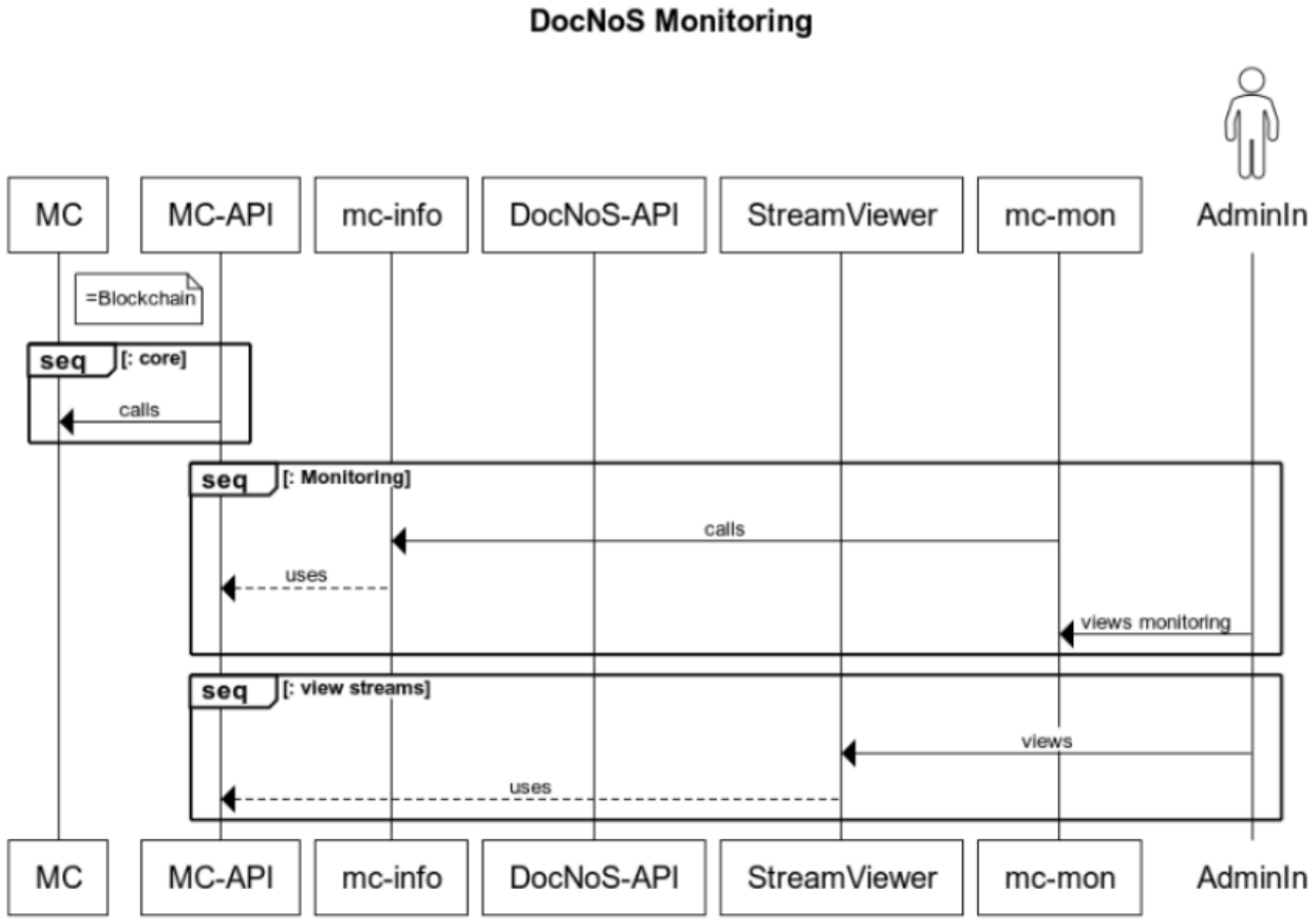
Blockhash	006afc51433905cc84a9ecfd0dd0dfbc502adadaedee245362e68db4decddea0
Blockzeit	2024-09-05T23:43:01+02:00
Bestätigungen	1732
Zeitstempel	2024-09-05T23:42:46+02:00
Hashwert (sha256)	04c6e09ff1e0df9621080ffb3c534fbb96fc07ef5db9533d5777f8d714bc03f1
Hashwert (sha512)	e1be022baa002ca294b20cd1a643620558eb4e36210a1028d8ca23fc466fed1d9 3e9b7c9bf2b92a7b1544a27937a9d301fad39425e81597355dabb312f45b1a6
Transaktions-ID	151e1e9466fc510783f144071409bac7b6152c9c3c927a95b722908441d9808d

AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

Monitoring

- mc-info
  - Serverprozesse
  - Sammeln Info der Node/s
- mc-mon/mc-view
  - Sammelt Infos der mc-infos
  - WebGUI: Darstellung
- Stream Viewer
  - Anzeige Inhalte der Streams



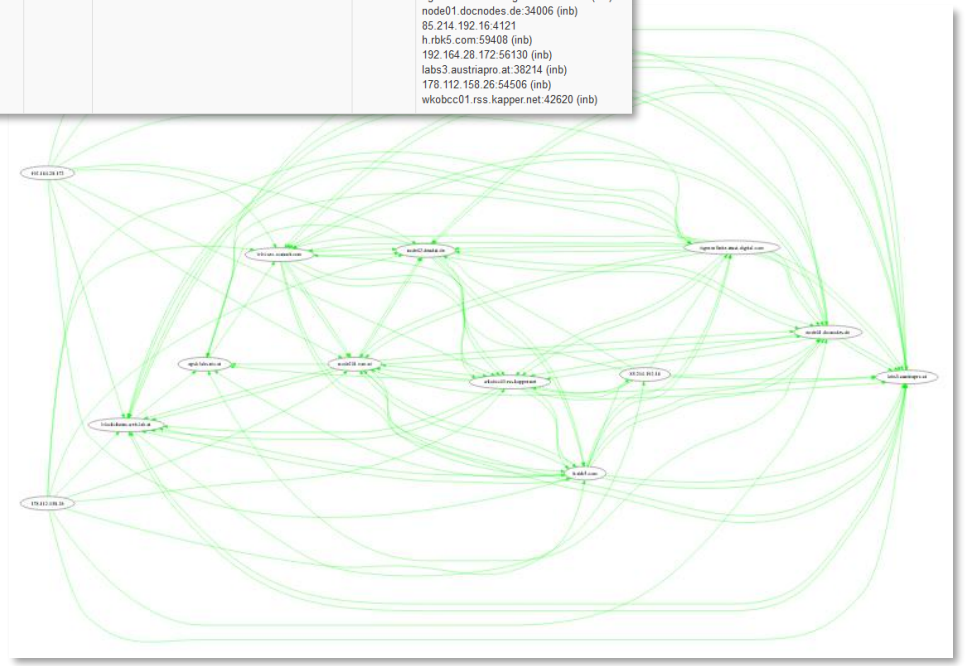
mc-view / Stream Viewer

Multichain Node(s) Status - NEU

blockchains.web-lab.at

ExtIP: 88.99.145.156, version: mc-info-pro v0.4, owner: baumann.at, dataUrl

chainname	version	blocks	nodeaddress	#conns	conns
datnos-c19	2.3.3	118383	datnos-c19@88.99.145.156:2683	6	bibi.sec-consult.com:2683 85.214.192.16:38996 (inb) h.rbk5.com:46184 (inb) 192.164.28.172:59204 (inb) labs3.austriapro.at:2683 178.112.158.26:54538 (inb)
datnos-20200220	2.3.3	487183	datnos-20200220@88.99.145.156:4121	10	apsb.labs.nic.at:4121 node201.ivm.at:56494 (inb) tiger.infinite-trust-digital.com:47794 (inb) node01.docnodes.de:34006 (inb) 85.214.192.16:4121 h.rbk5.com:59408 (inb) 192.164.28.172:56130 (inb) labs3.austriapro.at:38214 (inb) 178.112.158.26:54506 (inb) wkobcc01.rss.kapper.net:42620 (inb)



DocNoS - Data view

Select Key

[all] - bs-client-cb1 - bs-client-jb1 - dn-client-cb2 - dn-client-jb2 - dn-client-cb3 - dn-client-jb3 - proof.li - dn-client-cb4 - bibi.li - test.meinwko - ForFor - sha512: - sha3/512: - dn-client-v3-std - test.nic.at - dn-client-v3-std-KEY - test.securikett - cardid:123 - test.ma01.wien - dn-client-cb4-std - proof.li/c2 - proof.li/c2/test - sec/forfor/test - pyDemo - Blockstempel-v2 - ABC-Test1 - proof.li/c#-client/test - proof.li/csc/test - IVM/Test - Weinand/Test - digicert/test - digicert/mei - woschitz/test - ifm.tu/test - docnos/test - MTP/Test - condignum/Test - pydemo - dnfn/test - futurelab/Test - TelegramNotarizingBot/test - matdol/Test - icomedias/Test - itreebute/Test - vecctor.de/Test - artino/Test

Key: [all]

10 of 55049 items

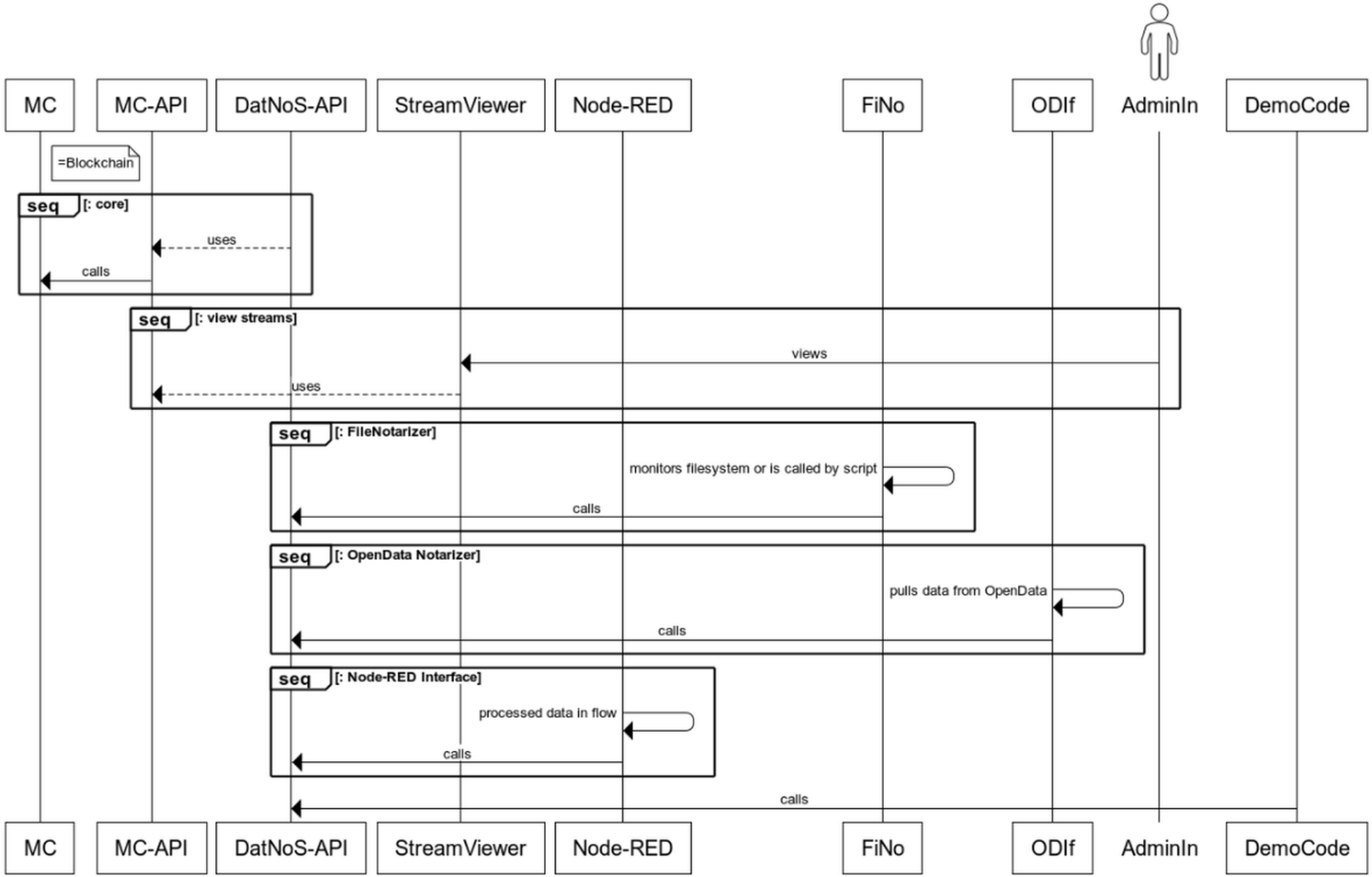
first - prev - next - last

Publishers	13VXwdarLRtV5fyP8qdWEFXebe6Ay45pgdY4Bb
Key 0	id:6d9b6745-0733-442d-91bc-7c789e7f2c23
Key 1	sha256:05a6fa5a397b24515eef50d830b5d242be551cc7f9ec296852e3dab9b12913dd
Key 2	sha512:76432dbb9051c0e8c8297743a85884db4575c2df0232bfe3ecf06ae0b2d848682084e478fbf356f852c1e0ed02edc3c1033600c9d3f312
Key 3	artino/Test
JSON data	{ "timeStamp": "2023-11-23T12:49:13+01:00", "client": "artino\/Test", "version": "DocNoS-v1.1", "data": { "id": "6d9b6745-0733-442d-91bc-7c789e7f2c23", "hashes": { "sha256": "05a6fa5a397b24515eef50d830b5d242be551cc7f9ec296852e3dab9b12913dd", "sha512": "76432dbb9051c0e8c8297743a85884db4575c2df0232bfe3ecf06ae0b2d848682084e478fbf356f852c1e0 }, "remarks": "CI_COMMIT_SHA" } }

AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

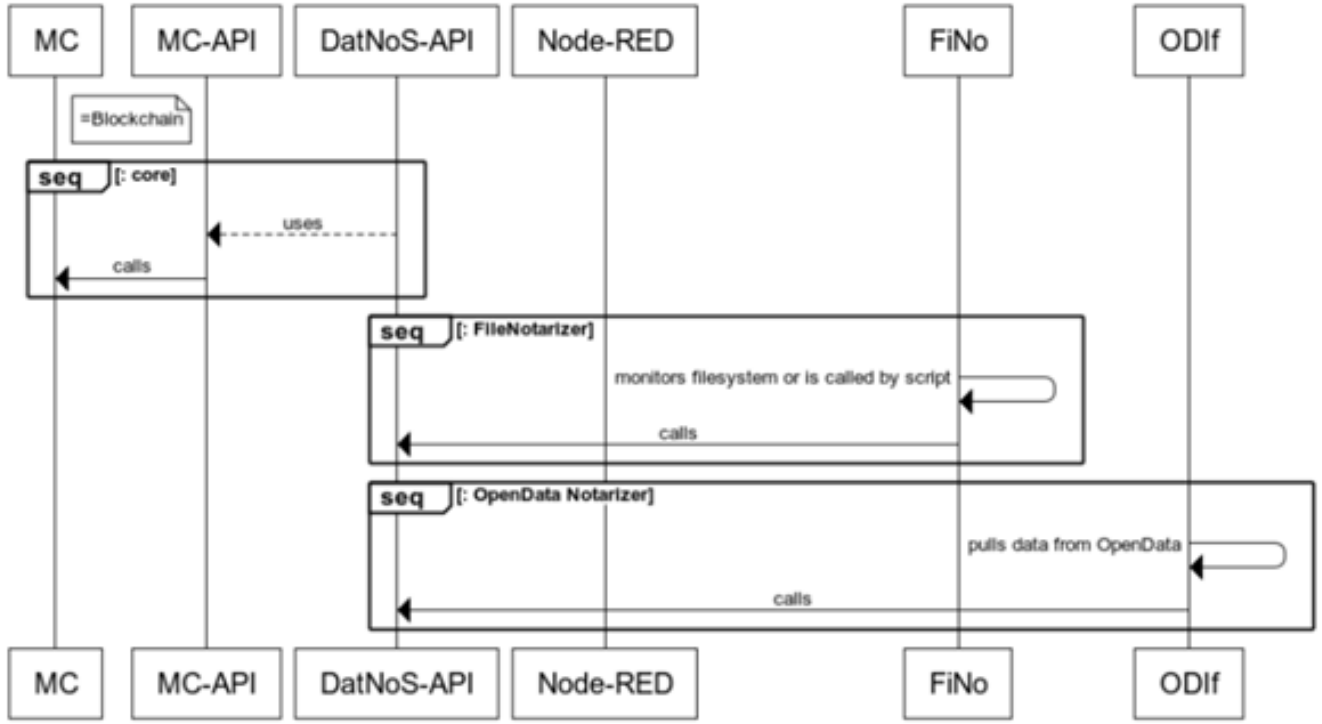
DatNoS Landscape & Artifacts



File/OpenData-Notarizer

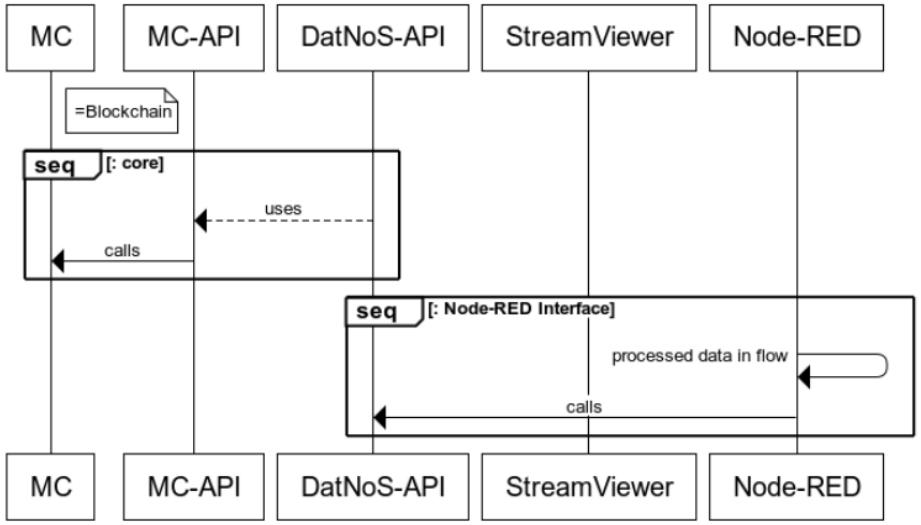
- Ähnlich zur DocNoS Version
- Speichert Daten in die Chain als
  - JSON
  - Binary

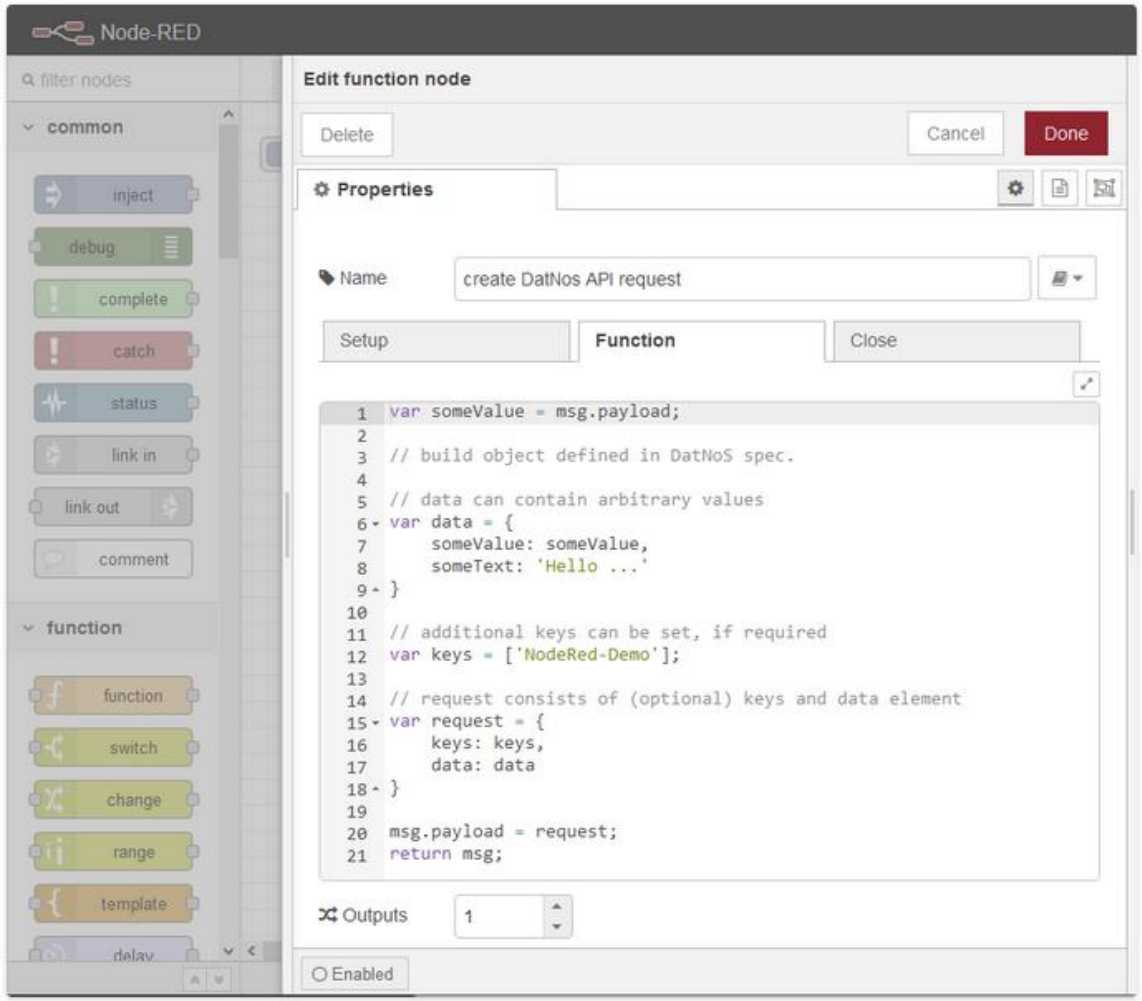
- Selbe Methode für „live“ Daten von
  - IoT devices
  - cloud services
  - …



Node-RED Interface

- … a flow-based, low-code development tool for visual programming
- Automation, IoT …





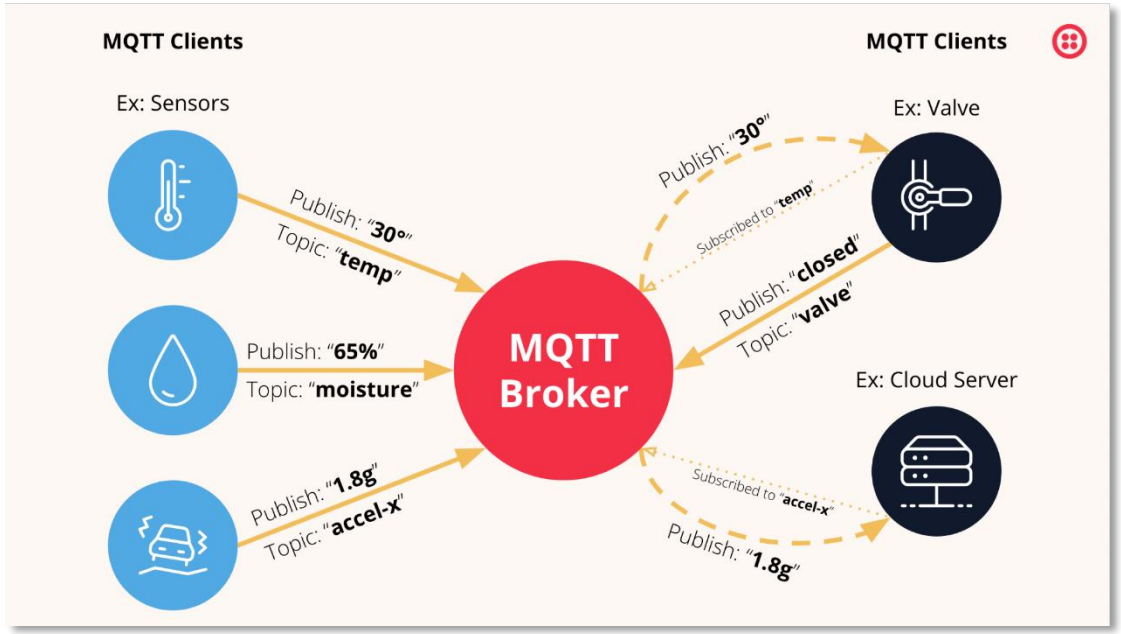
AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

Ansatz/Prototyp: Blockchain-Monitoring mit MQTT

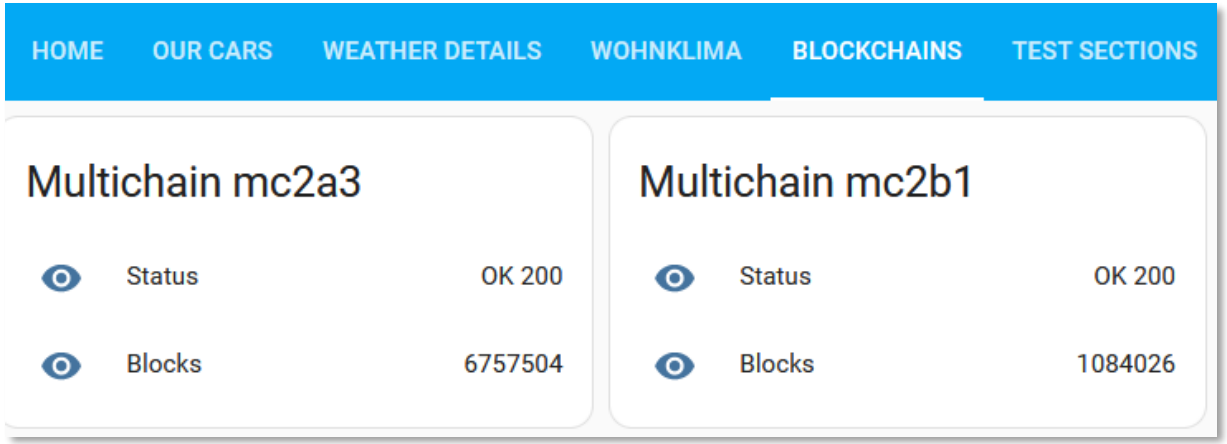
- MQTT: „Message Queuing Telemetry Transport“
- Einsatz ursprünglich im IoT Bereich (Sensoren, Aktoren …)
- Offenes Nachrichtenprotokoll
- „Kleinen Footprint“
  - Extrem schnelle Übermittlung, Speicherung, Abrufen von Daten
- Immer öfter auch im IT-Monitoring Bereich

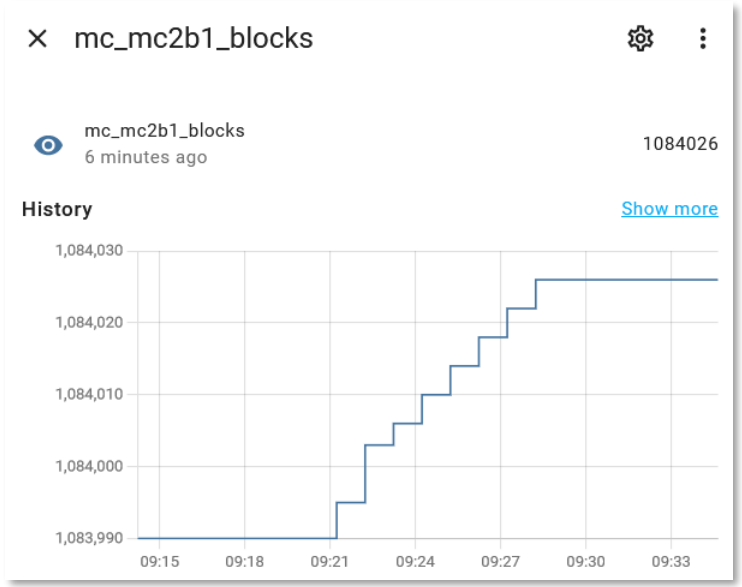
- https://www.twilio.com/en-us/blog/what-is-mqtt



Multichain-Monitoring Integration für Home-Assistant

- HA entwickelt für „Smart Home“
- Aber auch in anderen Umgebungen einsetzbar
- HA
  - „integration“ sammelt Infos der „mc-mon“ Module
  - Speichert sie in „Sensor-DB“
  - Anzeige auf Dashboards
- Next steps
  - InfluxDB, Grafana
  - MQTT …

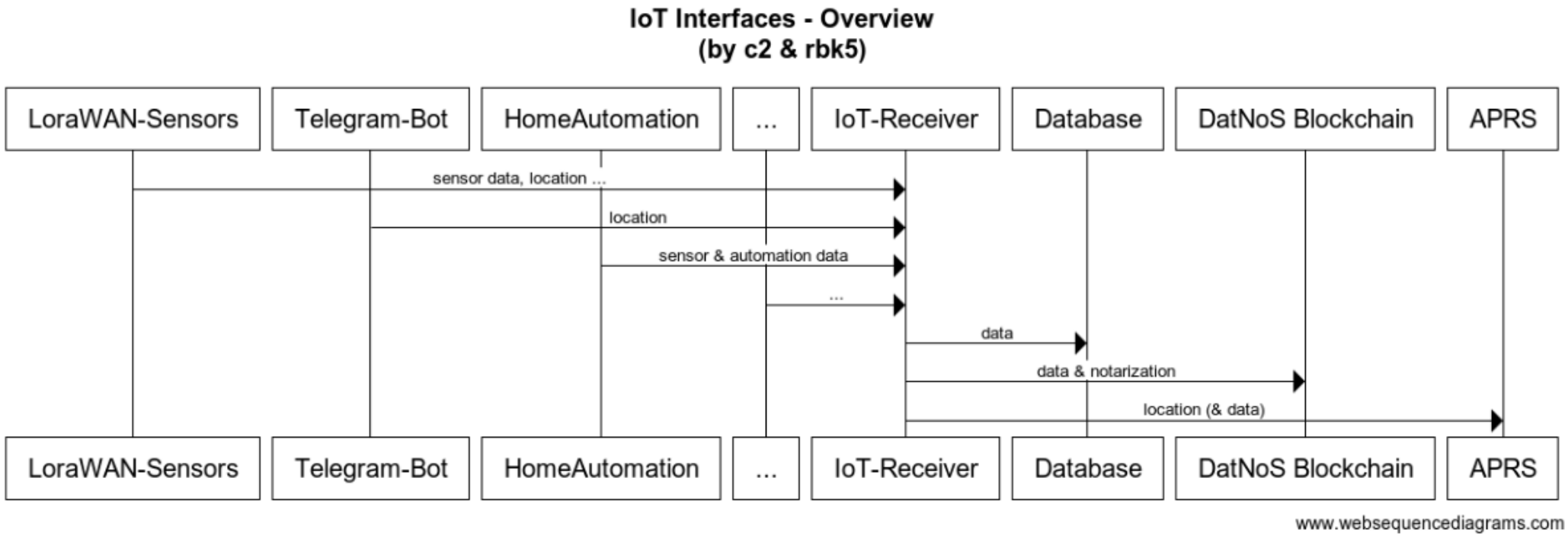




AUSTRIA PRO

BLOCKCHAIN INITIATIVE AUSTRIA

IoT Interfaces: Sensor -> Blockchain



Details siehe Präsentation Roman Bruckberger-Koch

Zusammenfassung

- Anwendung DocNoS
  - APSB, PSBC
  - User: WebGUI, Windows Client, (Telegram Bot)
  - Automatisierung: Files, OpenData, Git-Integration
  - Admin: Monitoring, Stream-Viewer
  - Demo-Code
- Anwendung DatNoS
  - Diverse Module verfügbar (Test, Prototyp)
  - Mehrere Usecases im Test
- Software-Module verfügbar
  - Produktion & Test, Prototypen
  - Quellen: AustriaPro-Lab & BC-Init (OpenSource), 3rd party
- Technische Kompetenz verfügbar
  - Installation/Betrieb Nodes, Implementierung, Security …