

# DocNoS/DatNoS

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

# 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)

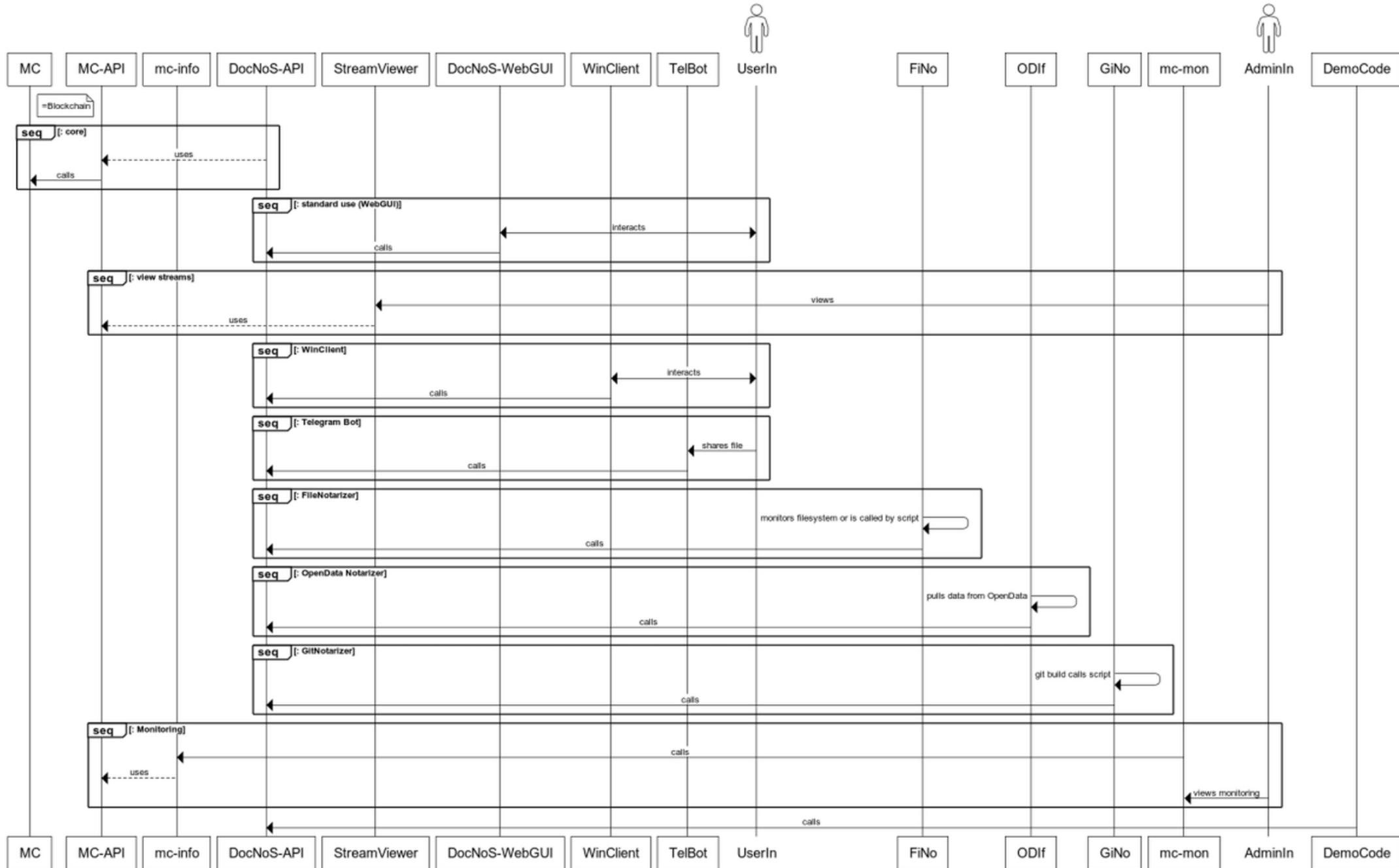
- [Web-GUI](#) für einen der im Lab installierten Blockchain-Nodes
- [Proof Of Existence - Demo](#)

### Node AustriaPro Lab 2 (ab 2023)

# DocNoS/DatNoS?

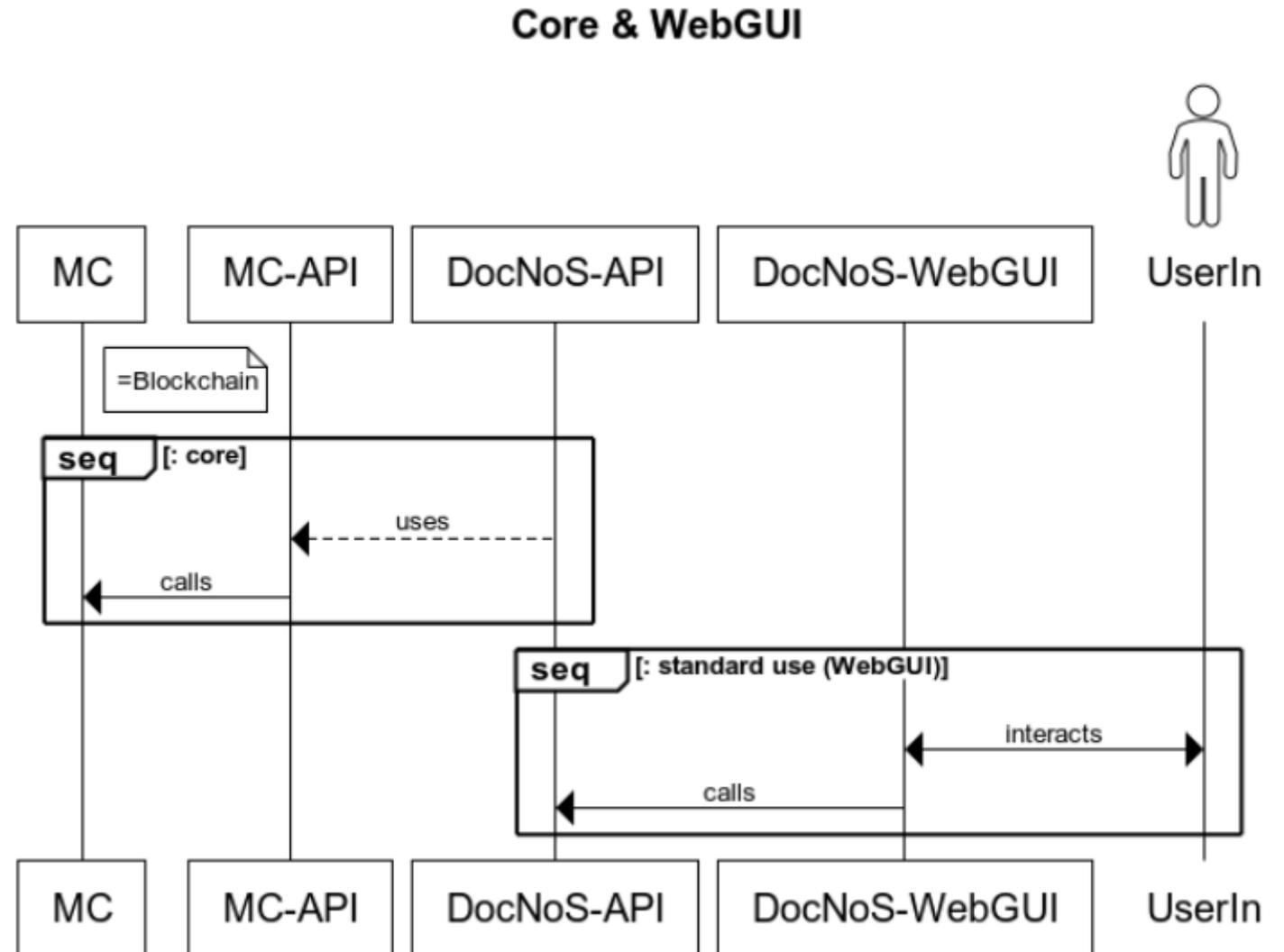
- DocNoS - Document Notarization Service
  - Speicherung von Hashwerten in der Blockchain
  - Daten sind/bleiben in der Usersphäre
  - Beispiele
    - Austrian Public Service Blockchain (WKO, WU, BMSGPK ...)
    - Private Sector Blockchain (Mitglieder Blockchain Initiative Austria)
- DatNoS - Data Notarization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

The screenshot shows the 'proof.li - Notarization' web interface. The browser address bar shows 'https://proof.li/?page=create'. The page has a header with the 'proof.li' logo and 'Create Verify' buttons. The main heading is 'Create notarization'. Below it, instructions state: 'To create a notarization, choose a document. The file is not uploaded to the server, the browser.' There are three input fields: 'Select file (will NOT be uploaded to the server):' with a file name 'Meeting\_CP132\_20220404.pdf', 'Calculated hash value (sha256):' with a long alphanumeric string, and 'Filename (\*):' with the same file name. A 'Remark (optional, \*):' field contains 'Report Meeting CP132'. A blue 'Create' button is at the bottom. At the very bottom, it shows 'Voucher-ID: 448737674, Transaction-Credits: 10'.

## Result of the creation

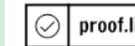


Notarization created.

The notarization was created successfully, details are shown in the following bottom of page).

<b>Time stamp</b>	2022-04-12T10:29:50+02:00
<b>Hash value</b>	5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6
<b>Transaction-ID</b>	5e3ec1ff4d390138efec0bbcf7f0fe0371cd32a6963b1
<b>Filename (*)</b>	Meeting_CP132_20220404.pdf
<b>Remark (*)</b>	Report Meeting CP132

(\*) for reference, will NOT be stored in the blockchain.



## Document Notarization - Certificate

Created at 12.04.2022 - 10:35:20

This is to certify, that the hash value ("SHA256") of the document was securely and immutably stored in the blockchain.

The following table shows all details:

Time stamp	2022-04-12T10:35:20+02:00
Hash value	5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6
Transaktions-ID	af282475078ca66e6f42dfdbb19850003ea8584d4205c961ac8e30c8f3471f04
Filename (*)	Meeting_CP132_20220404.pdf
Remark (*)	Report Meeting CP132

Data marked with (\*) is for information and reference only and not stored in the blockchain.

By using the following QR-Code or link you can invoke a verification service and pass the hash value.



<https://proof.li/?page=verify&fileHash=5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6>

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

# Notarization - Verification (Beispiel: Web-GUI)

## Verify notarization

Here you can check whether/when a document was notarized, i.e. the digital fingerprint (hash value) of a file was stored in the blockchain.

To do this, select the corresponding file (the hash value is calculated automatically), or enter

Select file (will NOT be uploaded to the server) to calculate hash value:

Meeting\_CP132\_20220404.pdf

or hash value (sha256):

or Transaction-ID:

The entered data is searched in the blockchain and displayed accordingly.

## Result of the verification



Hash value "5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6" found.

One entry was found, i.e. the document with the corresponding hash value was notarized in this system at the specified time.

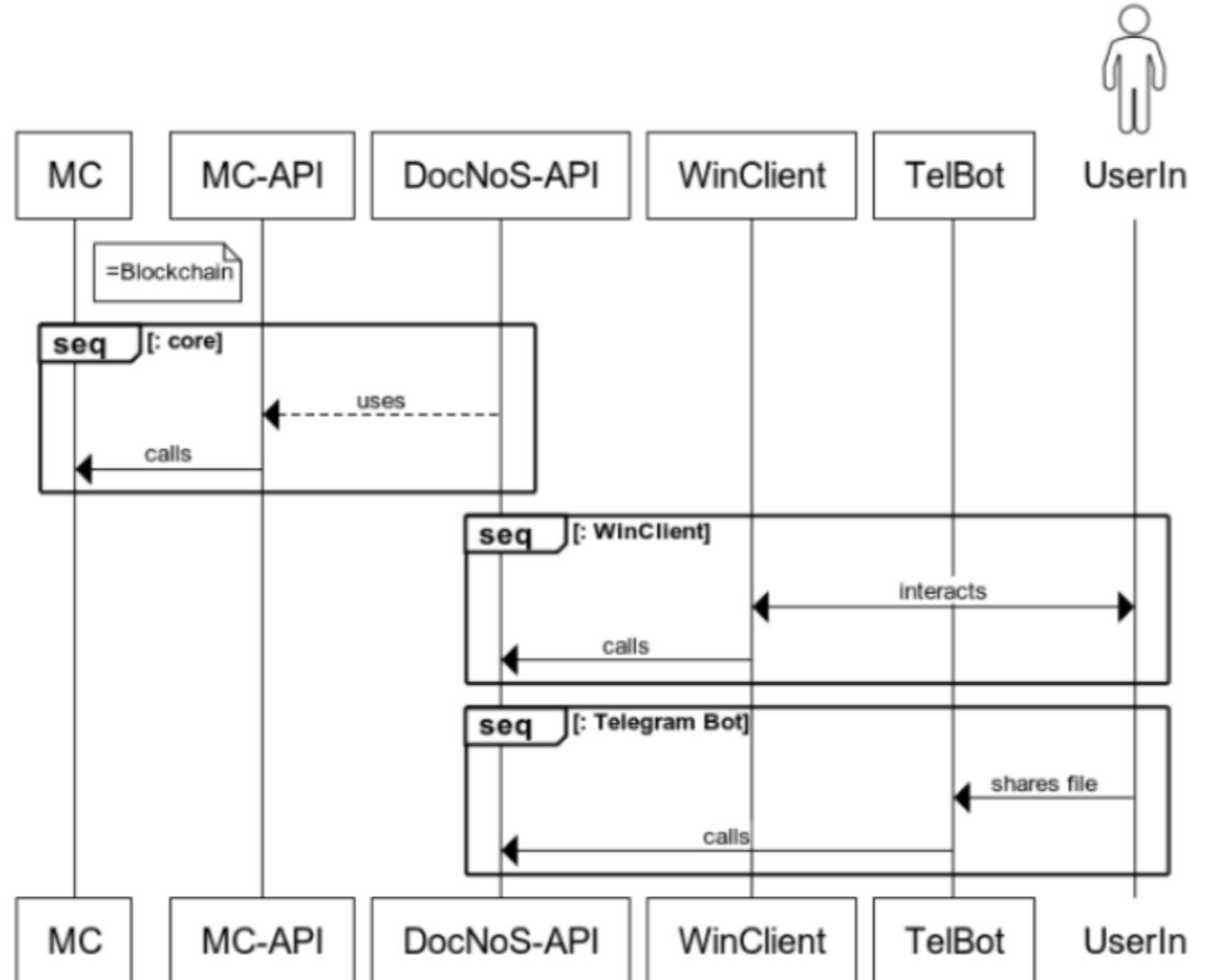
## Record 1/1

<b>Block hash</b>	0056149bdabd6f8635ca8393f7130aea9ac5d0728f0c0c42f3bf8f7a3097996b
<b>Block time</b>	2022-04-12T10:30:06+02:00
<b>Confirmations</b>	14
<b>Time stamp</b>	2022-04-12T10:29:50+02:00
<b>Hash value (sha256)</b>	5633b56f506b6f3199539ba956d75e5cd5ce5d1bdf18bec2b1357aedb45952e6
<b>Transaction-ID</b>	5e3ec1ff4d390138efec0bbcf7f0fe0371cd32a6963bb909a5742d578b209441

# Clients für User

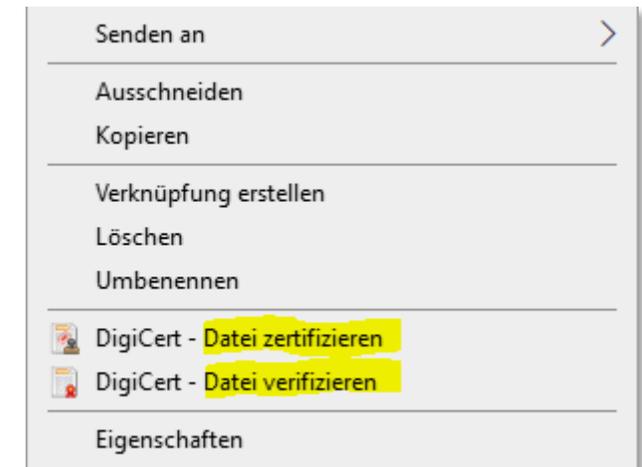
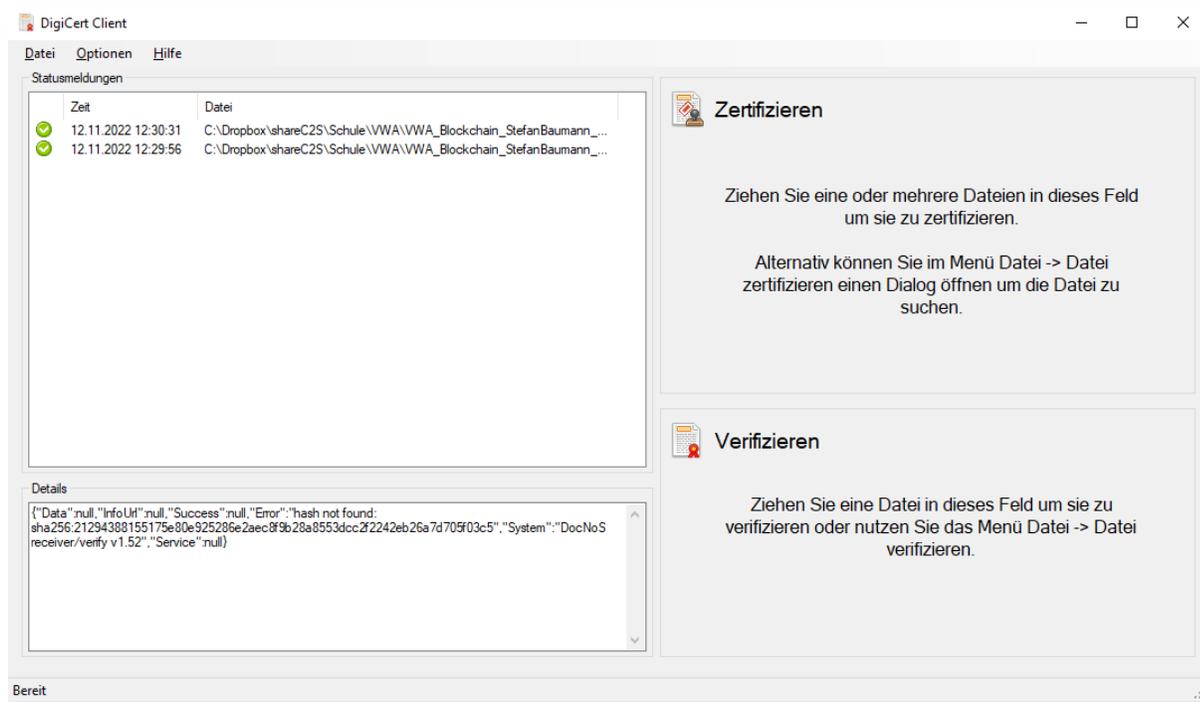
- Windows-Client
  - 3rd party
  - PSBC: mehrere Anwendungen
  - APSB: WU
- Telegram Bot
  - Prototyp auf Test-Chain

## DocNoS Clients for Users



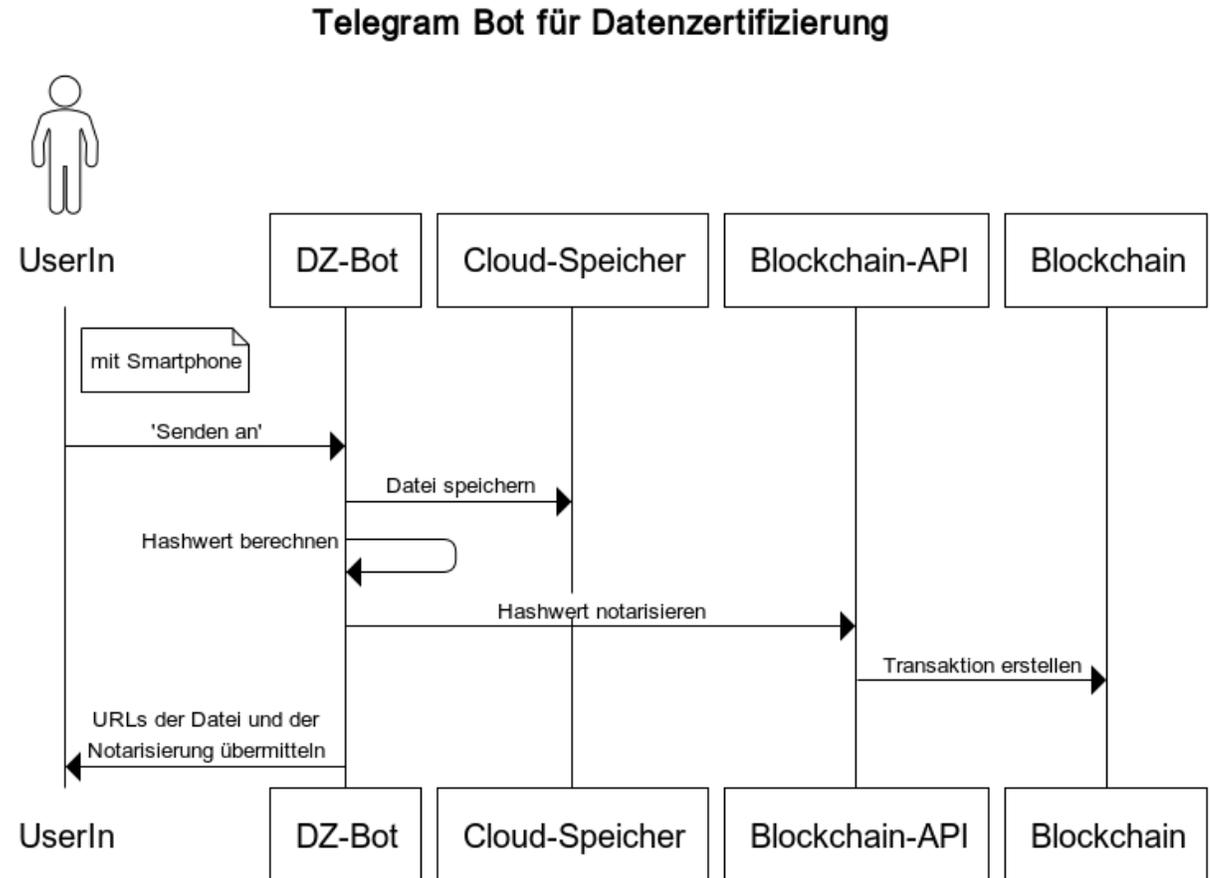
# DigiCert Client

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

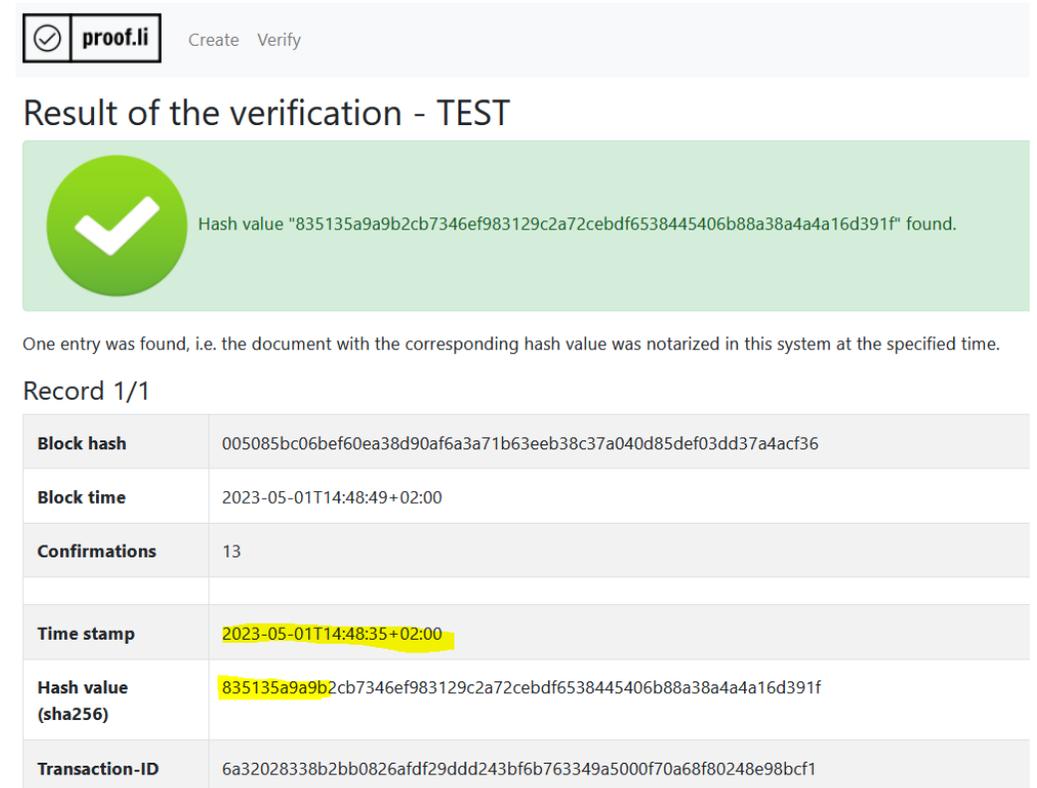
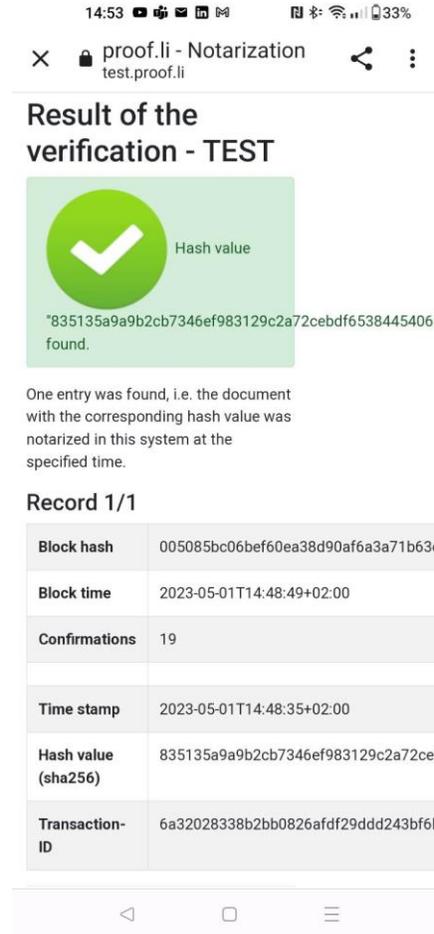
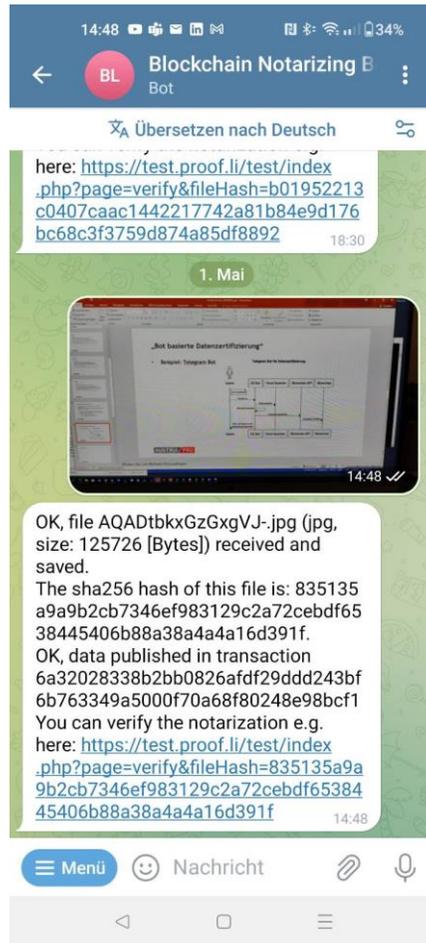


# „Bot basierte Datenzertifizierung“

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

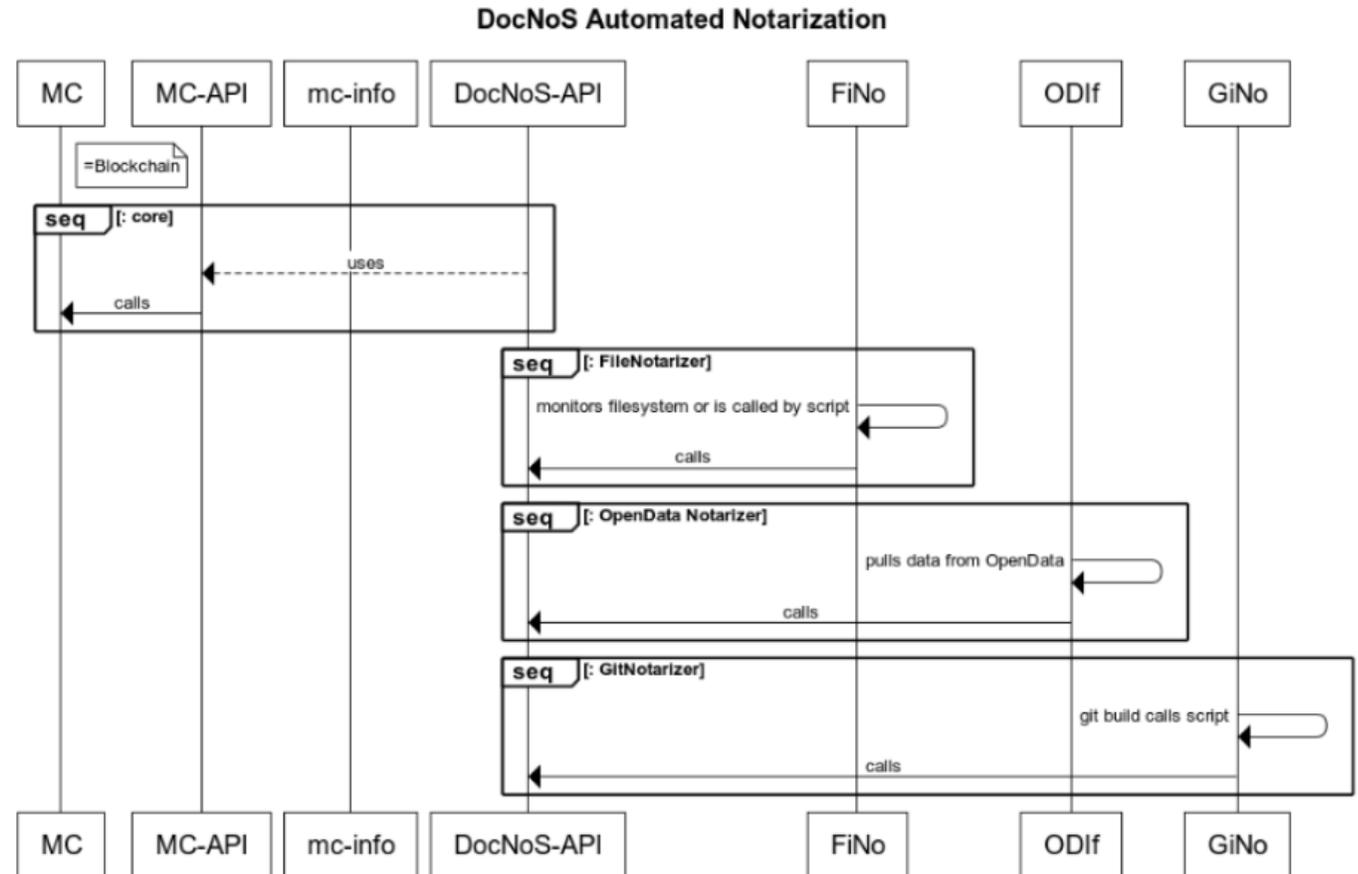


# Telegram Bot: „Blockchain Notarizing Bot“



# Automatisierte Notarisierung

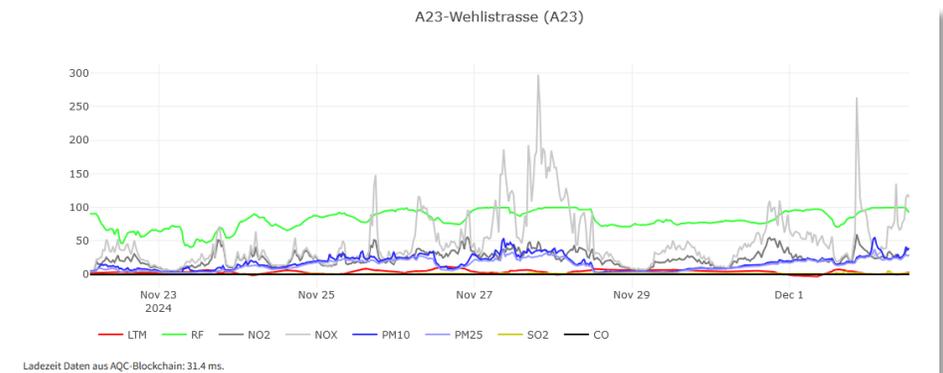
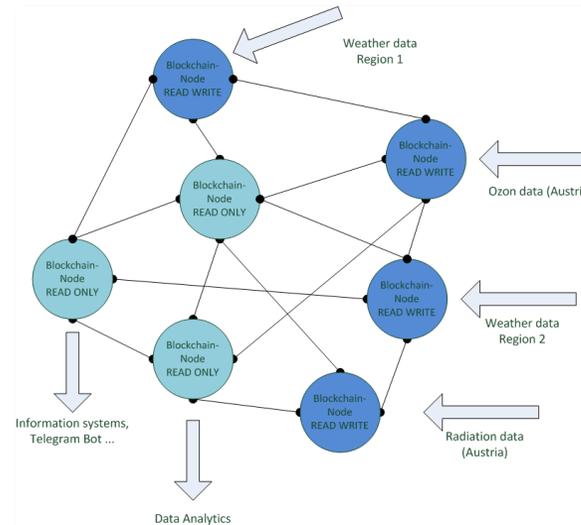
- File-Notarizer
  - ZB. BMSGPK
- OpenData Interface
  - Air Quality Chain
  - Wien OGD-Metadaten (in Entwicklung)
- Git-Notarizer
  - SW-Artetakte
  - In Build-Pipeline



# Beispiel AQC (Air Quality Chain)

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

Publishers	MC2.0a@FRA (1AW7CVnQwpkPvxM7Hun3EYzZKDZPIDNdpHSE3)
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 (1AW7CVnQwpkPvxM7Hun3EYzZKDZPIDNdpHSE3)
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 (1AW7CVnQwpkPvxM7Hun3EYzZKDZPIDNdpHSE3)
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

# 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“

```
4827 1026889 [INFO] -----
4828 1026889 [INFO] BUILD SUCCESS
4829 1026889 [INFO] -----
4830 1026889 [INFO] Total time: 17:05 min
4831 1026890 [INFO] Finished at: 2024-09-05T23:41:59+02:00
4832 1026890 [INFO] -----
4833 $ cp $CI_SCP_SCRIPT scp.sh && chmod +x ./scp.sh && ./scp.sh
4834 7.1.2
4835 $ cp $CI_DOCNOS_SCRIPT docnos.sh && chmod +x ./docnos.sh
4836 $ ./docnos.sh ./protocol-terminators/epsos-ncp-client/epsos-client-connector/target/openncp-client-connector-*.war
4837 % Total % Received % Xferd Average Speed Time Time Time Current
4838 Dload Upload Total Spent Left Speed
4839 100 768 100 399 100 369 189 174 0:00:02 0:00:02 --:--:-- 364
4840 {"success": "OK", "data published in transaction 151e1e9466f6c510783f144071409bac7b6152e9c3c927a95b722988441d9888d", "timeStamp": "2024-09-05T23:42:46+02:00", "id": "a2f153ad-e4e1-471d-804e-11a9208e687f", "txid": "151e1e9466f6c510783f144071409bac7b6152e9c3c927a95b722988441d9888d", "service": "DocNoS receiver\\create v1.6.2", "infos": {"client:artino\\Test v:1 stream:docnos-test-1 chain:mc2b1 rpc:127.0.0.1:7222"}} $ ./docnos.sh ./protocol-terminators/epsos-ncp-server/epsos-ws-server/target/openncp-ws-server-*.war
4841 % Total % Received % Xferd Average Speed Time Time Time Current
4842 Dload Upload Total Spent Left Speed
4843 100 761 100 399 100 362 172 156 0:00:02 0:00:02 --:--:-- 329
4844 {"success": "OK", "data published in transaction fdc82ddb7d50207362672ef7b105f64e4e1d22bb79f8c72dd35482be73da36b6", "timeStamp": "2024-09-05T23:42:50+02:00", "id": "bc9474fd-58af-4285-a142-986705c501e8", "txid": "fdc82ddb7d50207362672ef7b105f64e4e1d22bb79f8c72dd35482be73da36b6", "service": "DocNoS receiver\\create v1.6.2", "infos": {"client:artino\\Test v:1 stream:docnos-test-1 chain:mc2b1 rpc:127.0.0.1:7222"}} $ ./docnos.sh ./protocol-terminators/epsos-ncp-client/epsos-client-connector/target/openncp-client-connector-*.war
4845 % Total % Received % Xferd Average Speed Time Time Time Current
4846 Dload Upload Total Spent Left Speed
4847 100 768 100 399 100 369 482 446 --:--:-- --:--:-- 927
4848 {"success": "OK", "data published in transaction 7654355fd5fde915e574683f5c511f7f0b834d632cc993c67b92cb44b833c", "timeStamp": "2024-09-05T23:42:55+02:00", "id": "bd69194a-b778-4b4f-b4b4-796c47b327e7", "txid": "7654355fd5fde915e574683f5c511f7f0b834d632cc993c67b92cb44b833c", "service": "DocNoS receiver\\create v1.6.2", "infos": {"client:artino\\Test v:1 stream:docnos-test-1 chain:mc2b1 rpc:127.0.0.1:7222"}} $ ./docnos.sh ./protocol-terminators/epsos-ncp-server/epsos-nc-mock-it/target/openncp-nc-mock-it-*.jar
```

# Beispiel Git-Notarizer - Verifizierung

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

<b>Publishers</b>	13VxwdarLrtV5fyP8qdWFXe6eAy45pgdY4Bb
<b>Key 0</b>	id015f612d-381b-4efd-9a8e-899a6e4b1b25
<b>Key 1</b>	sha256:7fe38537b427b768c39e4111d7cf28c3cc7a7d524b89a0a3431fda4819b7bccd
<b>Key 2</b>	sha512:5cfd51d8a1e53d9b0017b445e07d6dd706b858fcb8bf1e9fcf5a0b48cfa315e572553a77bddabba489f617982cdee66abed46edd04cd0599ec736bce442ad8
<b>Key 3</b>	artino/Test
<b>JSON data</b>	<pre>{   "timeStamp": "2023-11-23T12:49:13+01:00",   "client": "artino/Test",   "version": "DoclioS-v1.1",   "data": {     "id": "015f612d-381b-4efd-9a8e-899a6e4b1b25",     "hashes": {       "sha256": "7fe38537b427b768c39e4111d7cf28c3cc7a7d524b89a0a3431fda4819b7bccd",       "sha512": "5cfd51d8a1e53d9b0017b445e07d6dd706b858fcb8bf1e9fcf5a0b48cfa315e572553a77bddabba489f617982cdee66abed46edd04cd0599ec736bce442ad8"     },     "remarks": "artifact openncp-configuration-utility-7.0.0.jar notarized by gitlab"   } }</pre>
<b>Transaction</b>	68f5817bfa14f2b6b11d17af381302115b772418e3ce296352b9904a88f229b
<b>Blocktime</b>	2023-11-23T12:49:25+01:00
<b>Blockhash</b>	002efbbd425bb3658b76a8157ae5728602dfd38b69085f599732b3a9673690b5
<b>Confirmations</b>	21

## Ergebnis der Verifikation - TEST



Hashwert "04c6e09ff1e0df9621080ffb3c534fbb96fc07ef5db9533d5777f8d714bc03f1" gefunden.

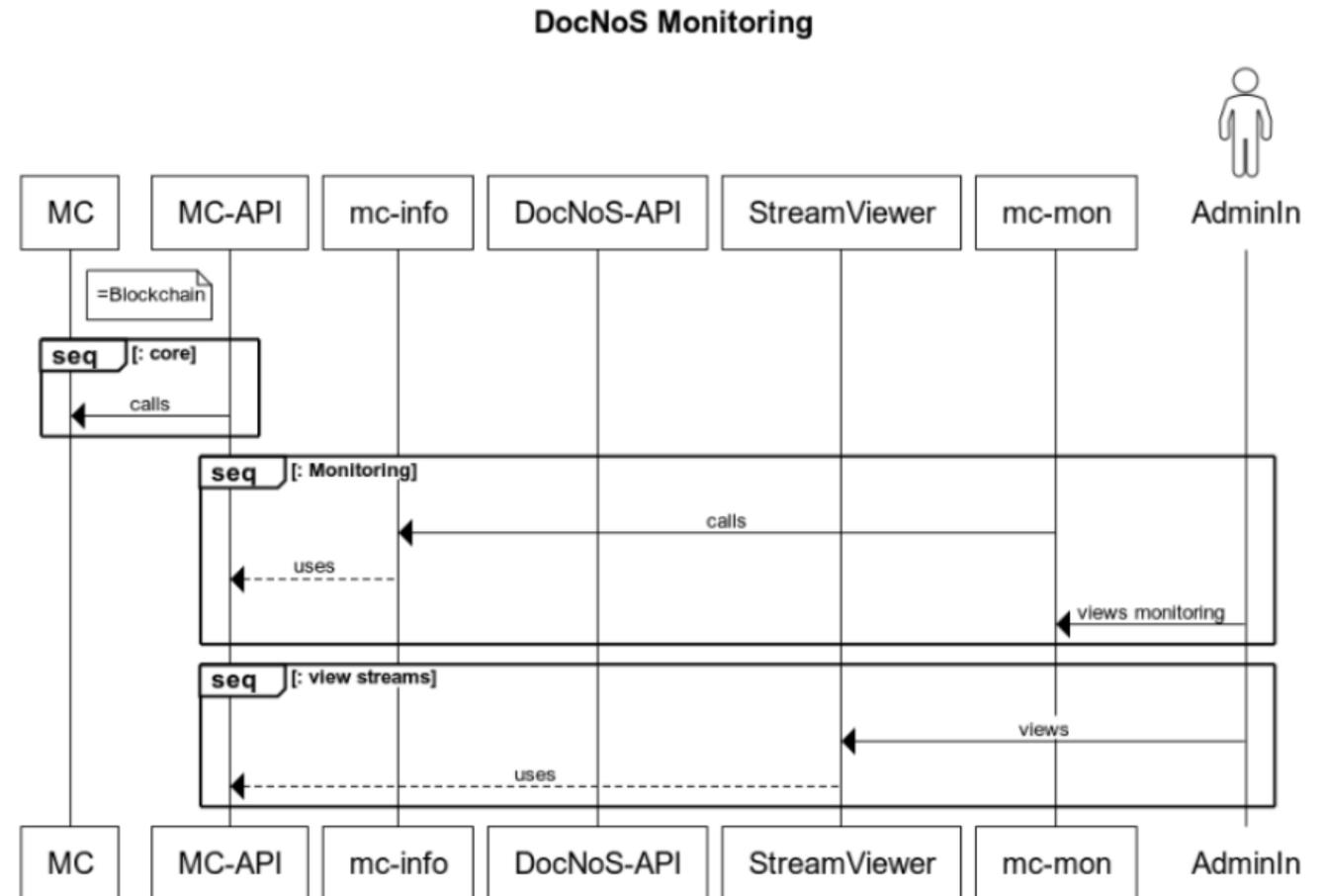
Es wurden mehrere Einträge gefunden, d.h. das Dokument wurde mehrfach notarisiert. Der älteste Eintrag (der erste in

### Eintrag 1/2

<b>Blockhash</b>	006afc51433905cc84a9ecfd0dd0dfbc502adadae245362e68db4decdea0
<b>Blockzeit</b>	2024-09-05T23:43:01+02:00
<b>Bestätigungen</b>	1732
<b>Zeitstempel</b>	2024-09-05T23:42:46+02:00
<b>Hashwert (sha256)</b>	04c6e09ff1e0df9621080ffb3c534fbb96fc07ef5db9533d5777f8d714bc03f1
<b>Hashwert (sha512)</b>	e1be022baa002ca294b20cd1a643620558eb4e36210a1028d8ca23fc466fed1d93e9b7c9bf2b92a7b1544a27937a9d301fad39425e81597355dabb312f45b1a6
<b>Transaktions-ID</b>	151e1e9466fc510783f144071409bac7b6152c9c3c927a95b722908441d9808d

# 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



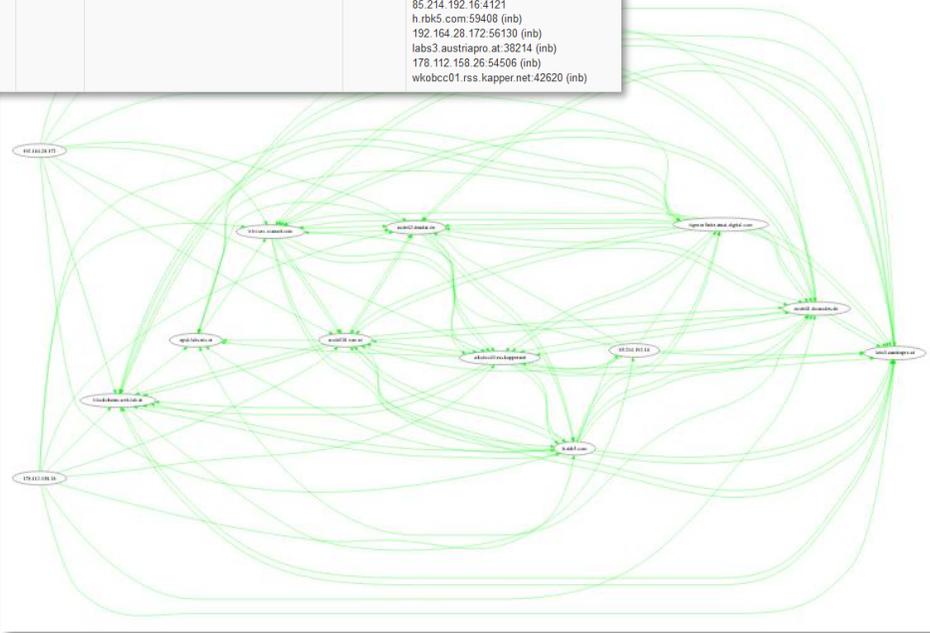
# mc-view / Stream Viewer

## 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 (mb) h.rbk5.com:46184 (mb) 192.164.28.172:59204 (mb) labs3.austriapro.at:2683 178.112.158.26:54538 (mb)
datnos-20200220	2.3.3	487183	datnos-20200220@88.99.145.156.4121	10	apsb.labs.nic.at:4121 node201.ivm.at:56494 (mb) tiger.infinite-trust-digital.com:47794 (mb) node01.docnodes.de:34006 (mb) 85.214.192.16:4121 h.rbk5.com:59408 (mb) 192.164.28.172:56130 (mb) labs3.austriapro.at:38214 (mb) 178.112.158.26:54506 (mb) wkobcc01.rss.kapper.net:42620 (mb)



## 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.nicat - 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 - dnf/test - futurelab/Test - TelegramNotarizingBot/test - matdol/Test - icomedias/Test - itreebute/Test - vecctor.de/Test - artino/Test

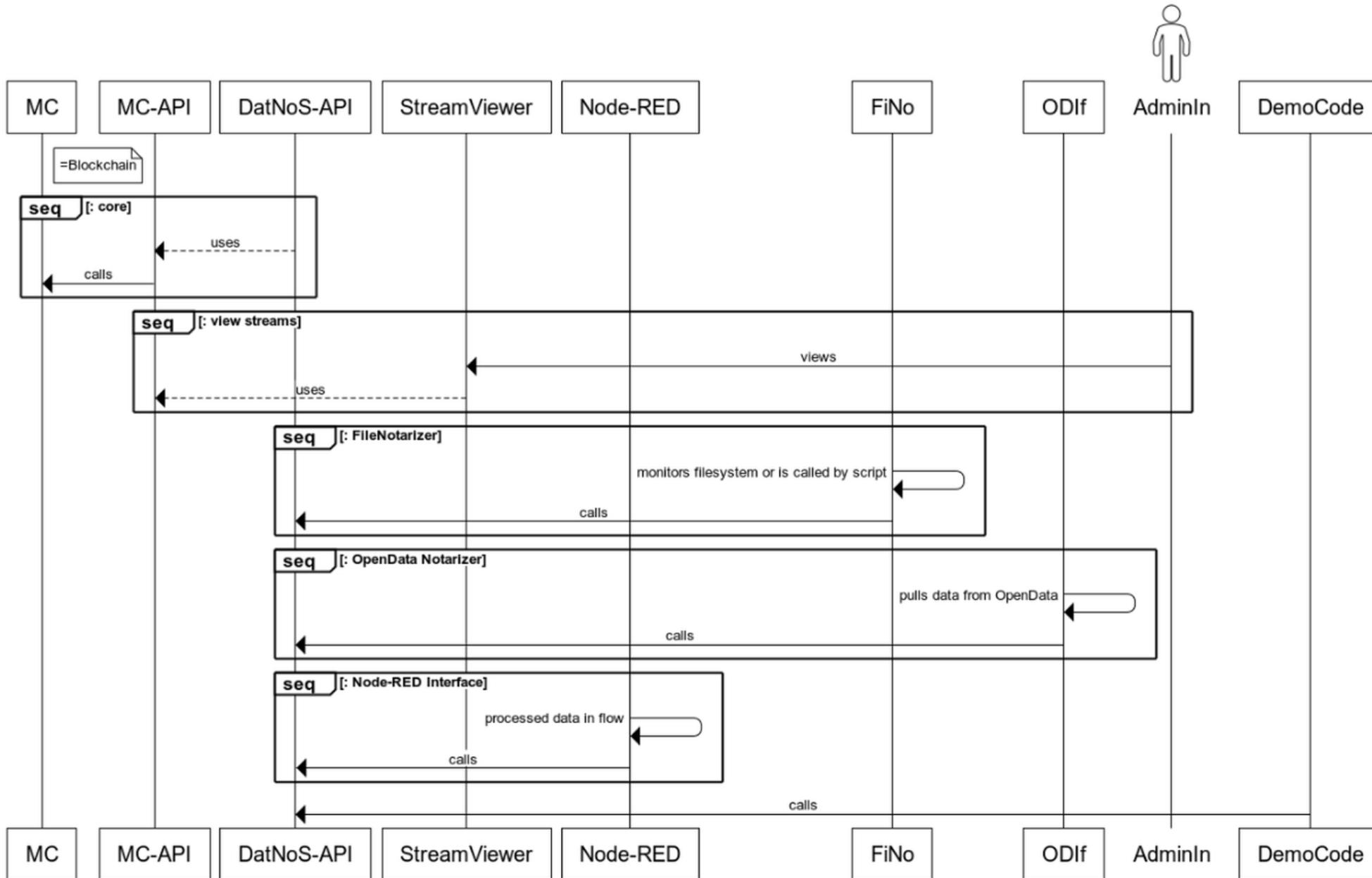
### Key: [all]

10 of 55049 items

first - prev - next - last

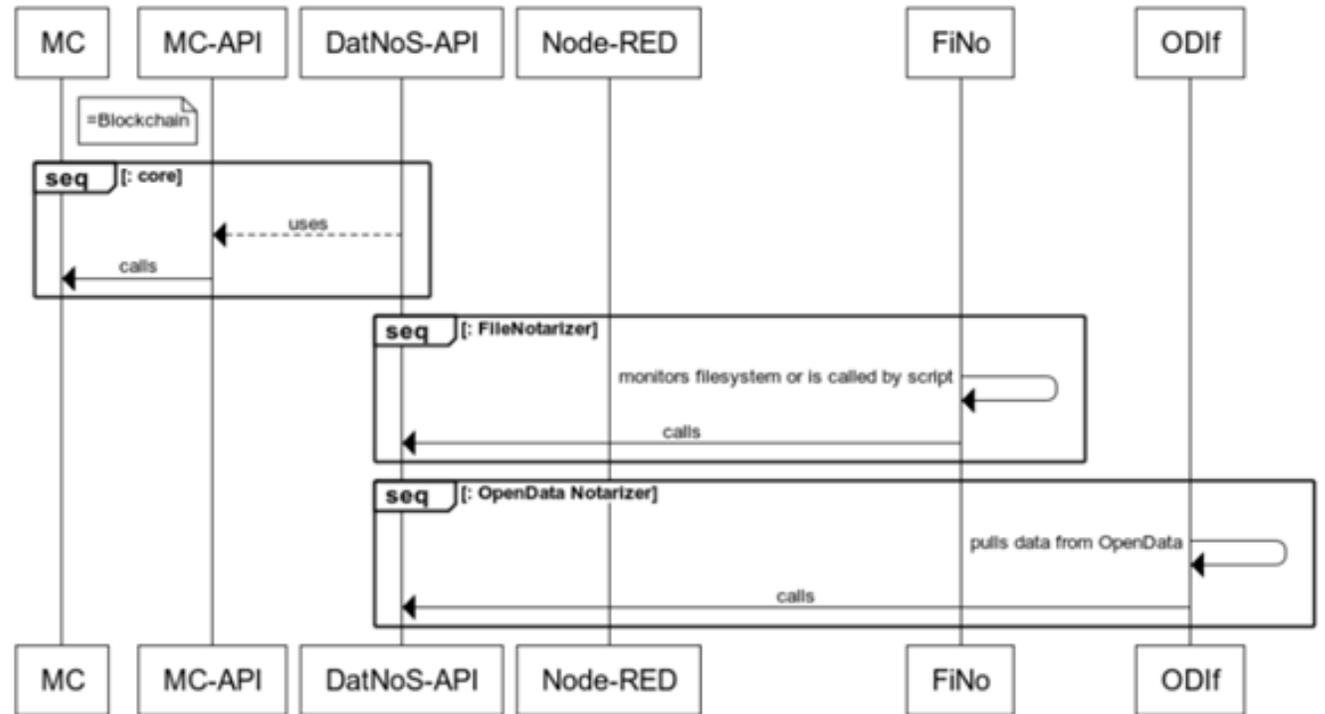
<b>Publishers</b>	13VXwdarLrtV5fyP8qdWEFxebe6Ay45pgdY4Bb
<b>Key 0</b>	id:6d9b6745-0733-442d-91bc-7c789e7f2c23
<b>Key 1</b>	sha256:05a6fa5a397b24515eef50d830b5d242be551cc7f9ec296852e3dab9b12913dd
<b>Key 2</b>	sha512:76432dbb9051c0e8c8297743a85884db4575c2df0232bfe3ecf06ae0b2d848682084e478fbf356f852c1e0ed02edc3c1033600c9d3f312
<b>Key 3</b>	artino/Test
<b>JSON data</b>	<pre>{   "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": "76432dbb9051c0e8c8297743a85884db4575c2df0232bfe3ecf06ae0b2d848682084e478fbf356f852c1e0e"     },     "remarks": "CI_COMMIT_SHA"   } }</pre>

# DatNoS Landscape & Artifacts



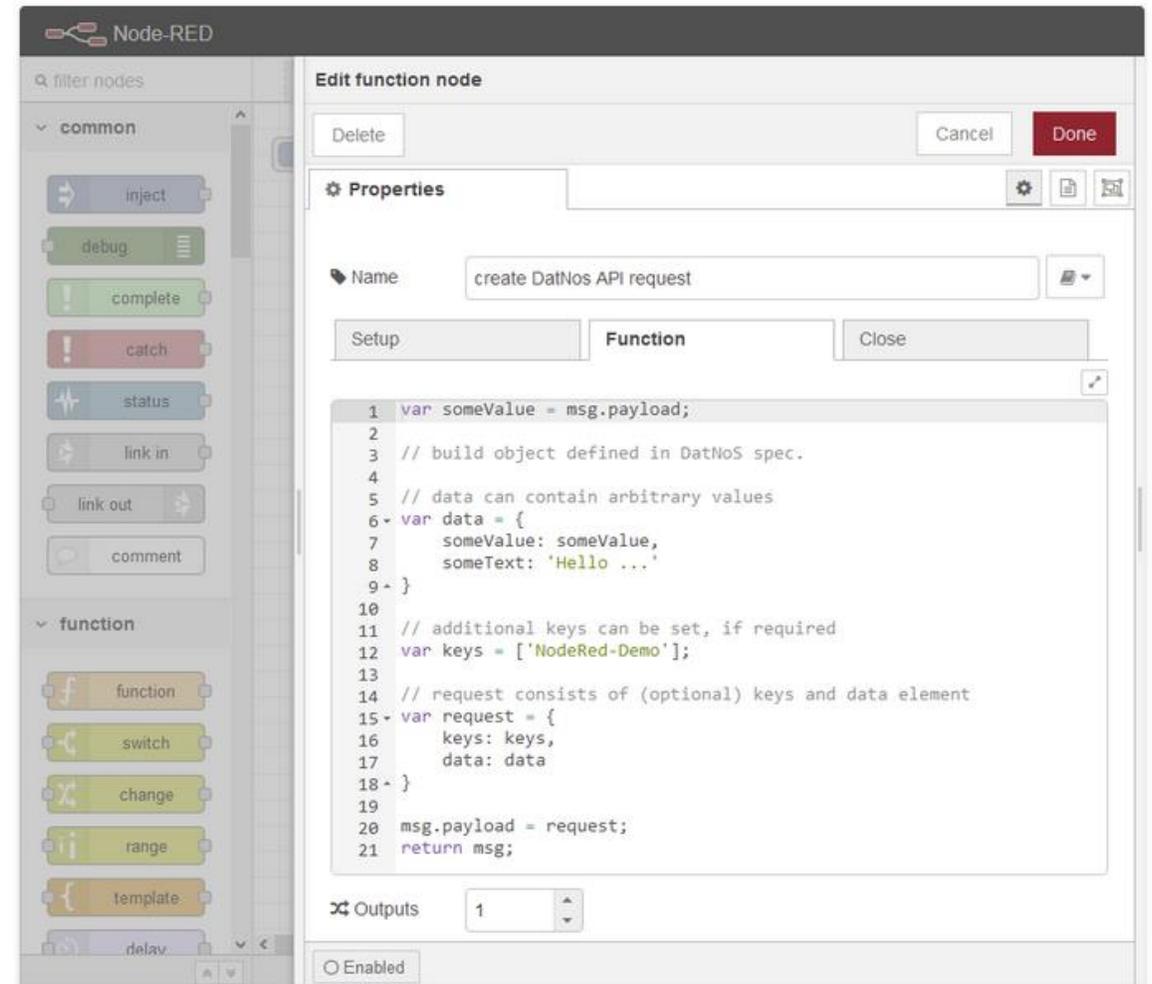
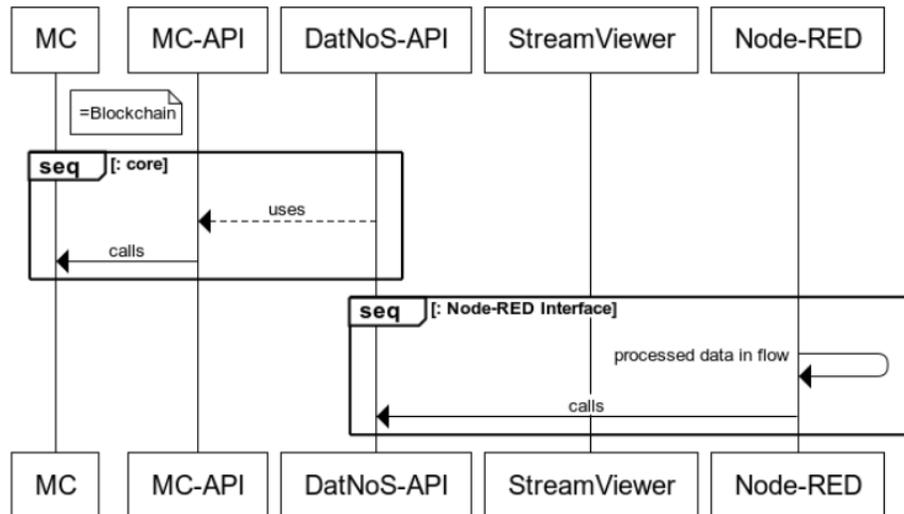
# File/OpenData-Notarizer

- Ähnlich zur DocNoS Version
- Speichert Daten in die Chain als
  - JSON
  - Binary
- Selbe Methode für „live“ Daten von
  - IoT devices
  - cloud services
  - ...



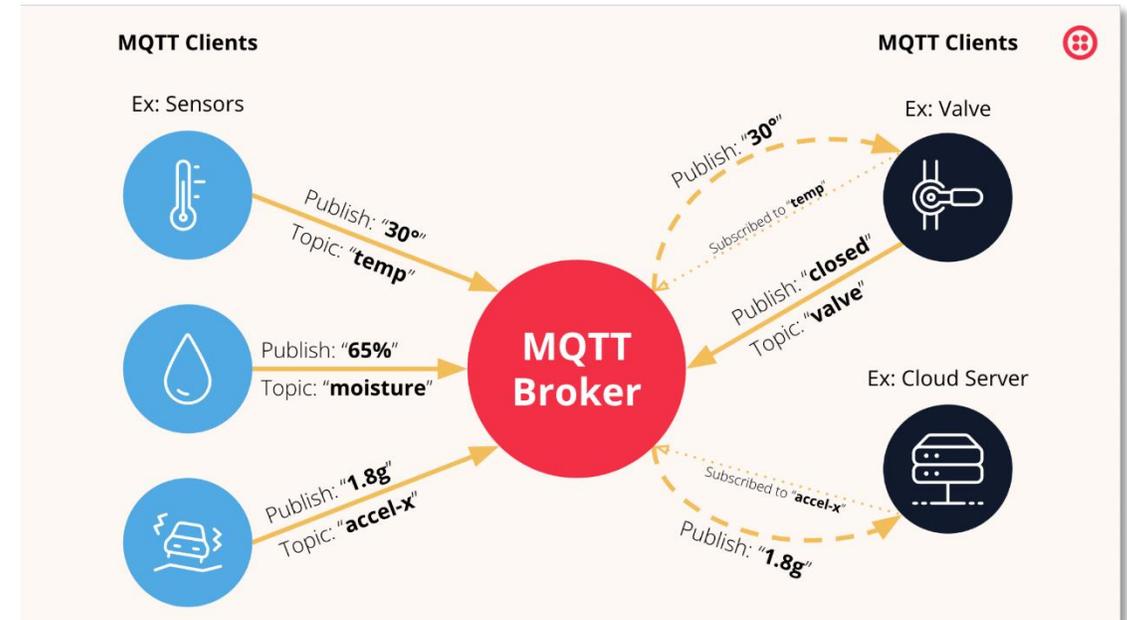
# Node-RED Interface

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



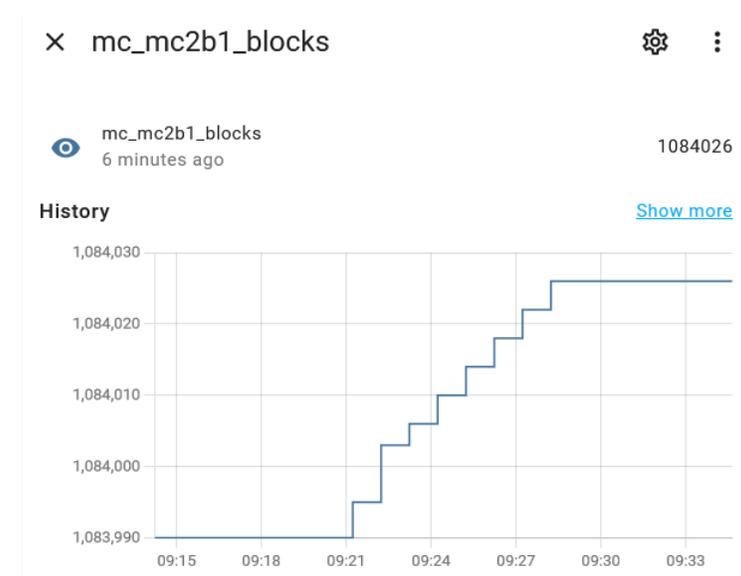
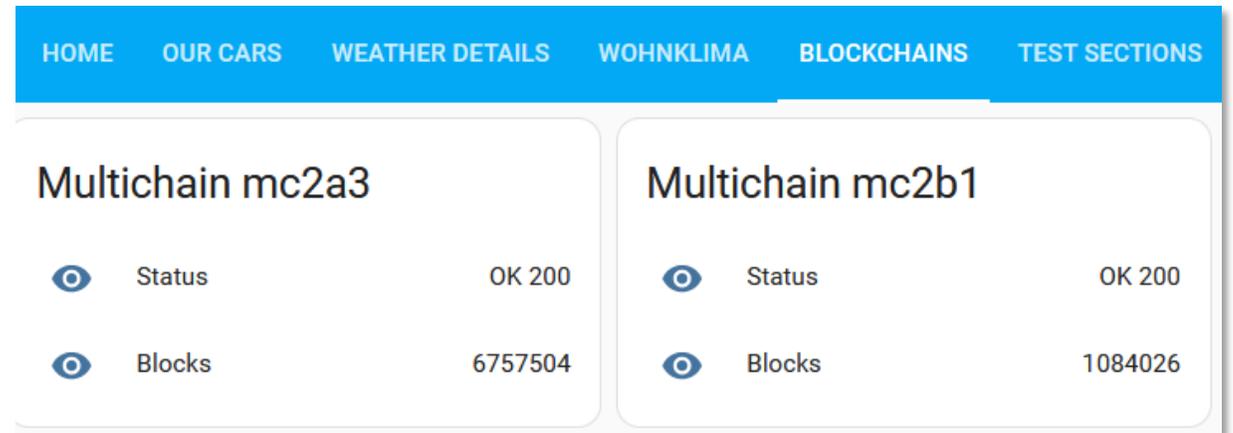
# Ansatz/Prototyp: Blockchain-Monitoring mit MQTT

- 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>



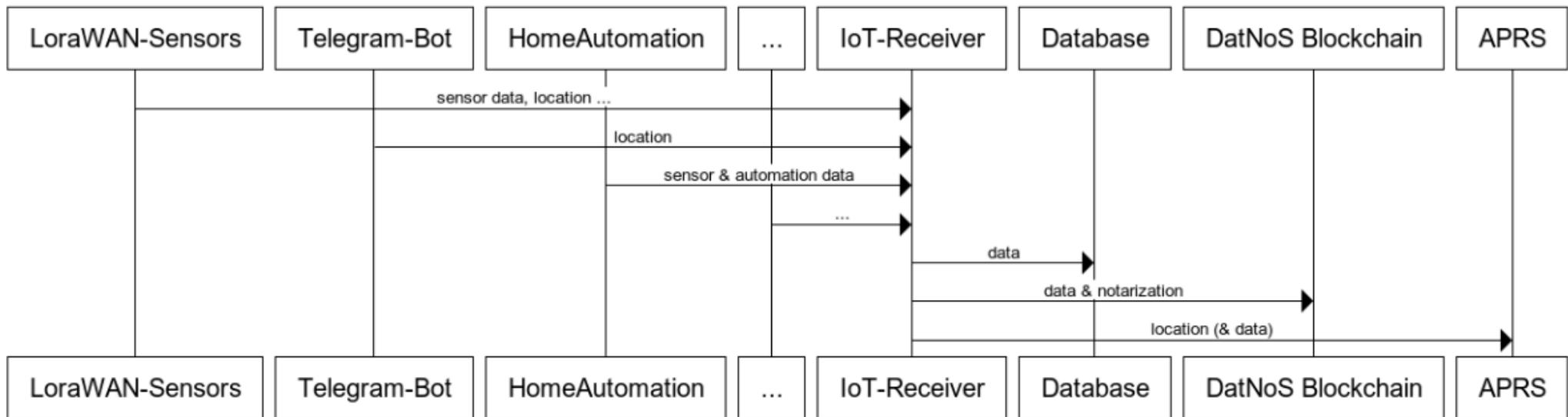
# Multichain-Monitoring Integration für Home-Assistant

- 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 ...



# IoT Interfaces: Sensor -> Blockchain

IoT Interfaces - Overview  
(by c2 & rbk5)



www.websequencediagrams.com

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 ...