# Arbeitskreis Blockchain
## Arbeitsgruppe Technik – Blockchain Lab
# Thema: Notarisierung

**AUSTRIAPRO**

**Dr. Christian Baumann**

**7.3.2019**

# Agenda – Notarisierung

- Überblick
- Testsystem Dokumenten-Notarisierung
  - Erstellen
    - PDF-Bestätigung
  - Verifizieren
- Technische Details
  - Systemaufbau
  - API-Beschreibung
- Next Steps

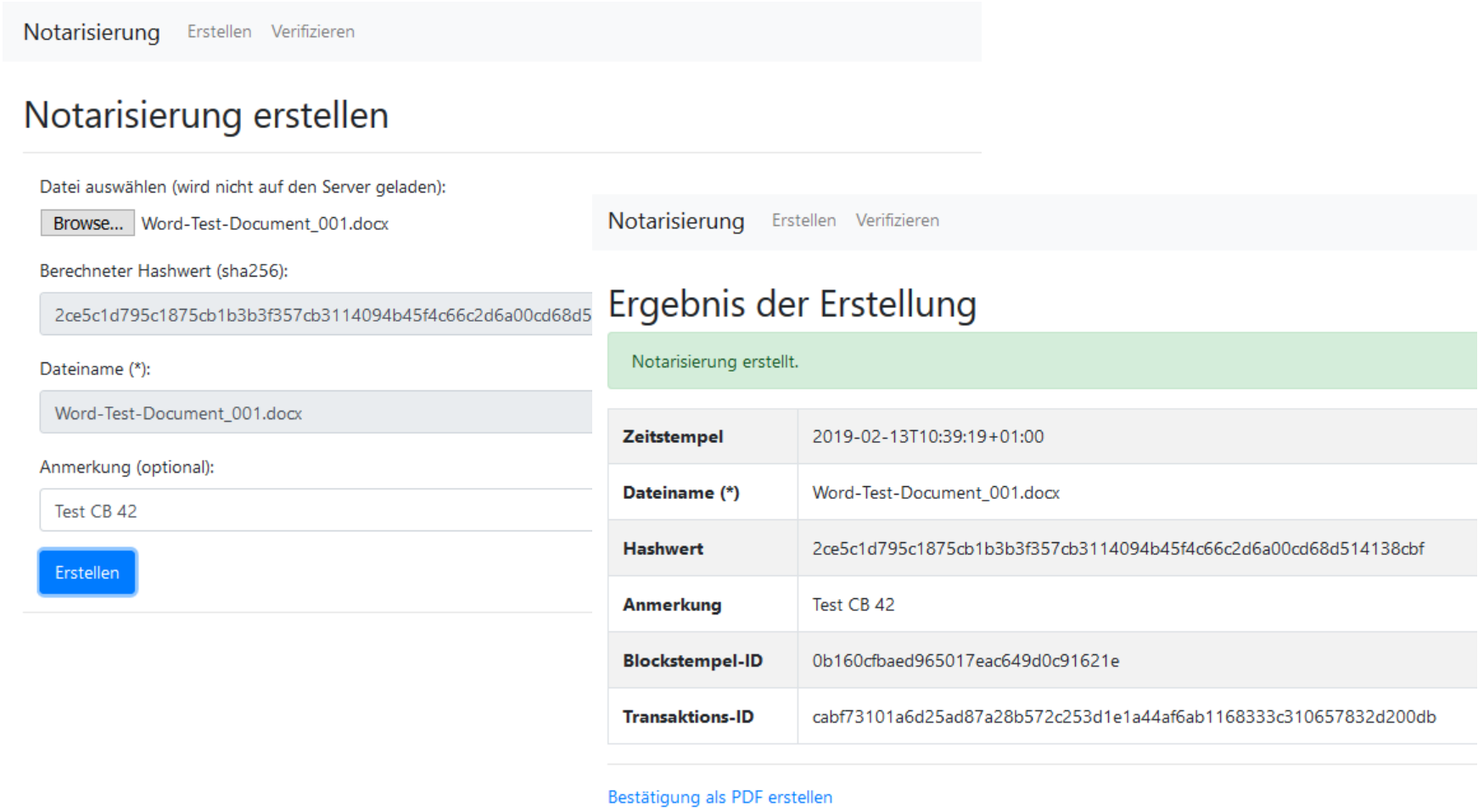
# Notarisierung – Überblick 1

- Notarisierung
  - Mit Notarisierung kann bewiesen werden, dass ein elektronisches Dokument zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert hat und seither nicht verändert wurde.
  - Die Sicherheit und das Vertrauen, dass hinterlegte Daten nicht manipuliert werden können, werden dabei durch die Blockchain-Technologie gewährleistet.
  - Es werden ausschließlich anonyme Daten verarbeitet!
    - Hashwerte von elektronischen Dokumenten
    - (ggf. technische Infos)
    - KEINE personenbezogenen Daten

# Notarisierung – Überblick 2

- Arbeitstitel „DocNoS“
  - Service, entwickelt im Auftrag der WKO, ist seit Anfang Februar 2019 im Testbetrieb.
  - Soll ab Mitte 2019 für alle WKO Mitglieder zur Verfügung stehen.
  - Und von der WKO zum Notarisieren von selbst erstellten Dokumenten genutzt werden.
  - Parallel dazu laufen Gespräche mit anderen Unternehmen und Institutionen, um ein Konsortium aufzubauen, um eine große gemeinsame Lösung auszuarbeiten und zu betreiben.

# Notarisierung - Erstellen



# Notarisierung – Bestätigung (PDF)

## Dokumenten Notarisierung - Bestätigung - TEST

### 13.02.2019 10:39:19

Zum angegebenen Zeitpunkt wurde der Hashwert eines Dokumentes in der "DocNoS" Blockchain hinterlegt. Folgende Tabelle zeigt Details dieser Transaktion:

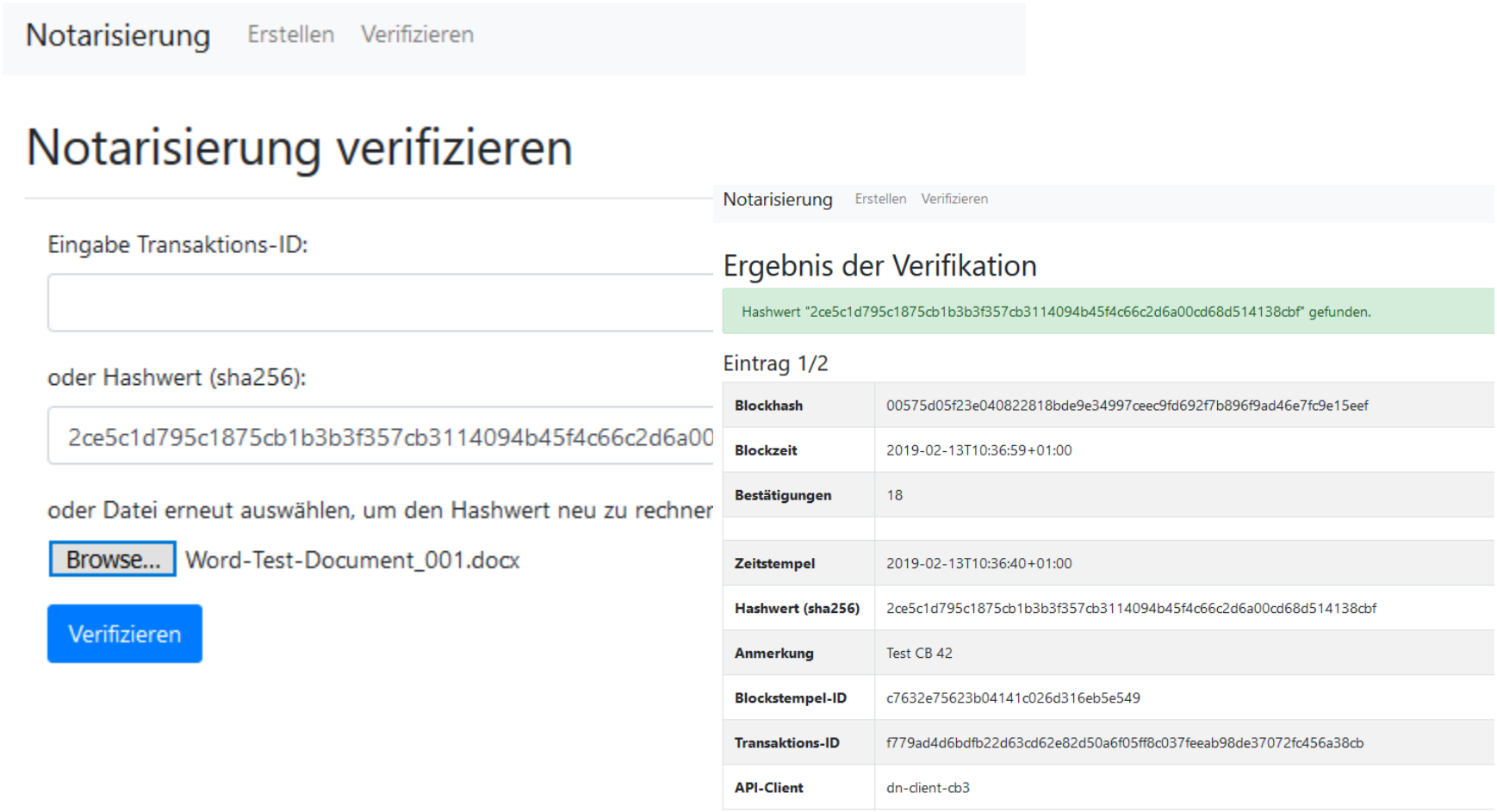
| | |
|---|---|
| Zeitstempel | 2019-02-13T10:39:19+01:00 |
| Dateiname (*) | Word-Test-Document_001.docx |
| Hashwert | 2ce5c1d795c1875cb1b3b3f357cb3114094b45f4c66c2d6a00cd68d514138cbf |
| Anmerkung | Test CB 42 |
| Blockstempel-ID | 0b160cfbaed965017eac649d0c91621e |
| Transaktions-ID | cabf73101a6d25ad87a28b572c253d1e1a44af6ab1168333c310657832d200db |

Die mit (*) markierten Daten wurden nicht in der Blockchain gespeichert, sie dienen nur zur Information.

Mit folgendem QR-Code bzw. Link kann die Transaktions-ID an ein Verifikationsservice übergeben werden.

Verifikationsservice (beim Öffnen mit QR-Codeleser bitte Adresse beachten!)
https://blockchains.web-lab.at/docnos/?page=verify&txid=cabf73101a6d25ad87a28b572c253d1e1a44af6ab1168333c310657832d200db

# Notarisierung - Verifizieren

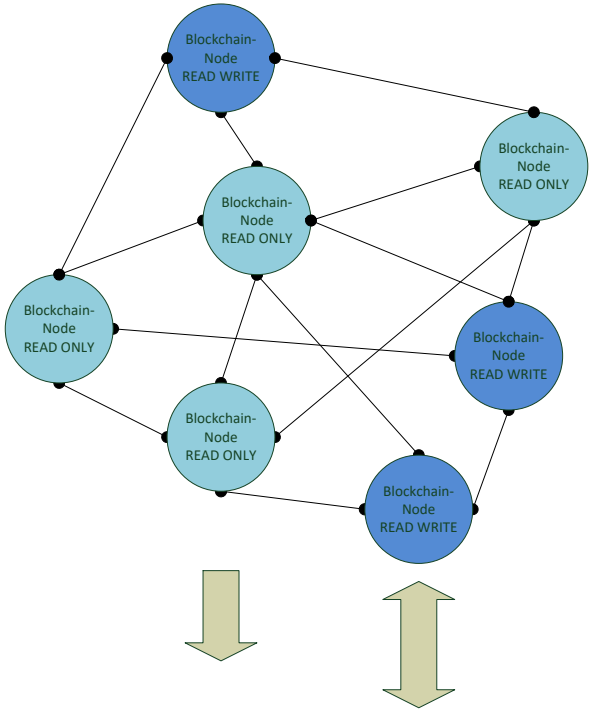


# Technik – Systemaufbau

- Testsystem
- Plattform: MultiChain 2.0
  - Opensource GPLv3
  - Alternativ kommerzielle Lizenz (incl. SLA)
- Sicherheit
  - Zwingend https
    - `Web-GUI -> API`
    - `Clients -> API`
    - `API -> Blockchain-Node`
  - Optional VPN
    - `API -> Blockchain-Node`

# Systemaufbau - Teilnehmer

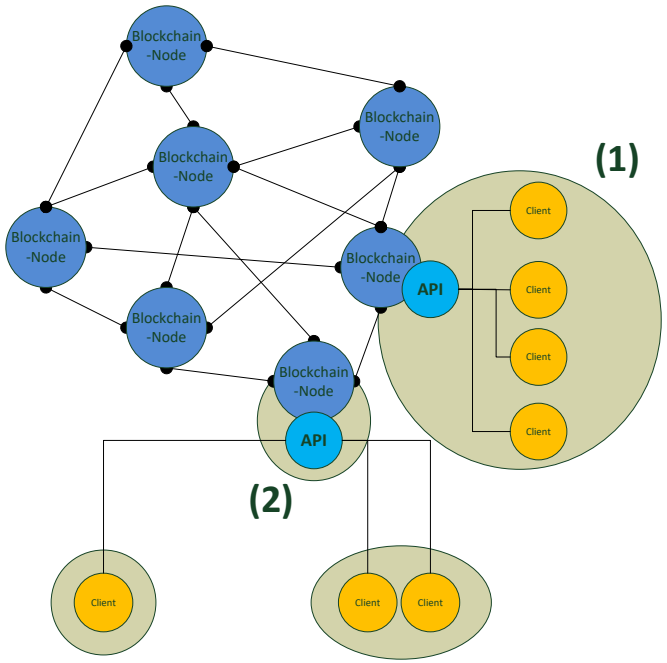
- Rollen
  - Lese/Schreibzugriff: „Institutionen*“, die API anbieten
    - Für deren Kunden und/oder
    - Eigene Anwendungen
  - Lesezugriff
    - Für „unabhängige Stellen“, die „Verifikation“ anbieten




(*) Konsortialmitglieder, Partner …

# Systemaufbau - APIs

- Mögliche Ausprägungen
  - Eigener Node und API (1)
  - Node und API von Dienstleister (2)
  - Mischformen (Node und API getrennt)



# REST-API - Notarisierung erstellen

- Url: https://labs2.austriapro.at/docnos-api/create/
- Authentifizierung mit http-Header
  - X-ApiToken: 123…TOKEN…123
- Nutzdaten in JSON – Request (POST)

```
{
	"hashes": {
		"sha256":
"099ff8e8d814c2291fd2e0726b37ff659ae48d88d86f2711e10d8421701adbd0",
		"sha512":
"7d76663b2e498cbdc11d192702ce1b547e4401f232cb848973afa893a9dbdc7929f614693f01d91577
540b6c5383e4233e780f0bfcc0d50d81f4332266c54f08"
	},
	"remarks": "an OPTIONAL remark"
}
```

# REST-API - Notarisierung erstellen

- Response


```
{
	"success": "OK, data published in transaction
dd5d6ddd0ade06a2ef6b67af01ef0bf86f64507781b063c33afd23ea957da606",
	"timeStamp": "2019-01-28T12:06:00+01:00",
	"id": "259bc390182462824de0606d00950c47",
	"txid": "dd5d6ddd0ade06a2ef6b67af01ef0bf86f64507781b063c33afd23ea957da606",
	"service": "DocNoS receiver/create v0.1"
}
```


Im Fehlerfall wird folgender Response gesendet:

| Statuscode | Bedeutung |
|---|---|
| 401 | Kein (gültiges) API-Token gesetzt |
| 405 | Method not allowed: Request ist kein Post-Request |
| 400 | Bad request:<br>• Keine Nutzdaten vorhanden oder Nutzdaten nicht (korrekt) JSON codiert<br>• Kein Element „hashes“ in den Nutzdaten |
| 500 | Fehler in der Konfiguration des Services |

# REST-API - Notarisieung verifizieren

- Url: https://labs2.austriapro.at/docnos-api/verify/
- GET oder POST Request
  - Parameter (hash oder id)
    - „hash“ in der Form „type:value“, z.B. `sha256:f24fa7d9333a3f40314c2f00dd28e0e706997819e66efe19619433dae285f3a3`
    - „txid“, z.B. `0a73bcf89842fc6d92dc5088005f04bd6bc8ae9e50eb45da9e1d9ed88370770c`
    - „id“
- Response


```
{
      "success": "OK, data published in transaction
dd5d6ddd0ade06a2ef6b67af01ef0bf86f64507781b063c33afd23ea957da606",
      "timeStamp": "2019-01-28T12:06:00+01:00",
      "id": "259bc390182462824de0606d00950c47",
      "txid": "dd5d6ddd0ade06a2ef6b67af01ef0bf86f64507781b063c33afd23ea957da606",
      "service": "DocNoS receiver/create v0.1 "
}
```

# Abbildung in Blockchain-Stream

| | |
|---|---|
| **Publishers** | 1HGyj7dBtX3SR43hqcpJAcrAi2TjX8nH4AN7Qf |
| **Key 0** | b541519fe6f8ce8a1cd16ef3fea64cb9 |
| **Key 1** | sha256:b9b4c0b3029e12552737e98d8fdbecbf8feaa0a69bf54383cf1364862c5c2dde |
| **Key 2** | sha512:06c23b6abe1d78d7959fb6f95938cc513bb441de27b27ecef6fc1099df10a5a66bdaee6b11a292ff2 |
| **Key 3** | bs-client-jb1 |
| **JSON data** | {<br>"timeStamp": "2019-01-30T09:15:30+01:00",<br>"client": "bs-client-jb1",<br>"data": {<br>"id": "b541519fe6f8ce8a1cd16ef3fea64cb9",<br>"hashes": {<br>"sha256": "b9b4c0b3029e12552737e98d8fdbecbf8feaa0a69bf5438<br>"sha512": "06c23b6abe1d78d7959fb6f95938cc513bb441de27b27ec<br>}<br>}<br>} |
| **Added** | 2019-01-30 08:15:35 GMT (confirmed) |
| **Data location** | on-chain, available |

# Next Steps

- Organisatorisch
  - „Konsortium“
    - Gespräche zwischen WKO, BRZ, Kontrollbank, Wien
  - „Rulebook“
    - => im Laufen …
- Technisch
  - Teilnahme am Testsystem
    - GUI: Url siehe Labs-Homepage
    - Anbindungen APIs: API-Token auf Anfrage
    - Eigener Node & API
- Zu erledigen
  - Abstimmung (& Verfeinerung) Spezifikation
  - Lasttests

# Kontakt

AUSTRIAPRO

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

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