

# **Blockchain im Digitalen Wien**

## **Technologie einer innovativen Verwaltung**

November 2017

Magistratsdirektion der Stadt Wien  
Geschäftsbereich Organisation und Sicherheit  
Gruppe Prozessmanagement und IKT-Strategie

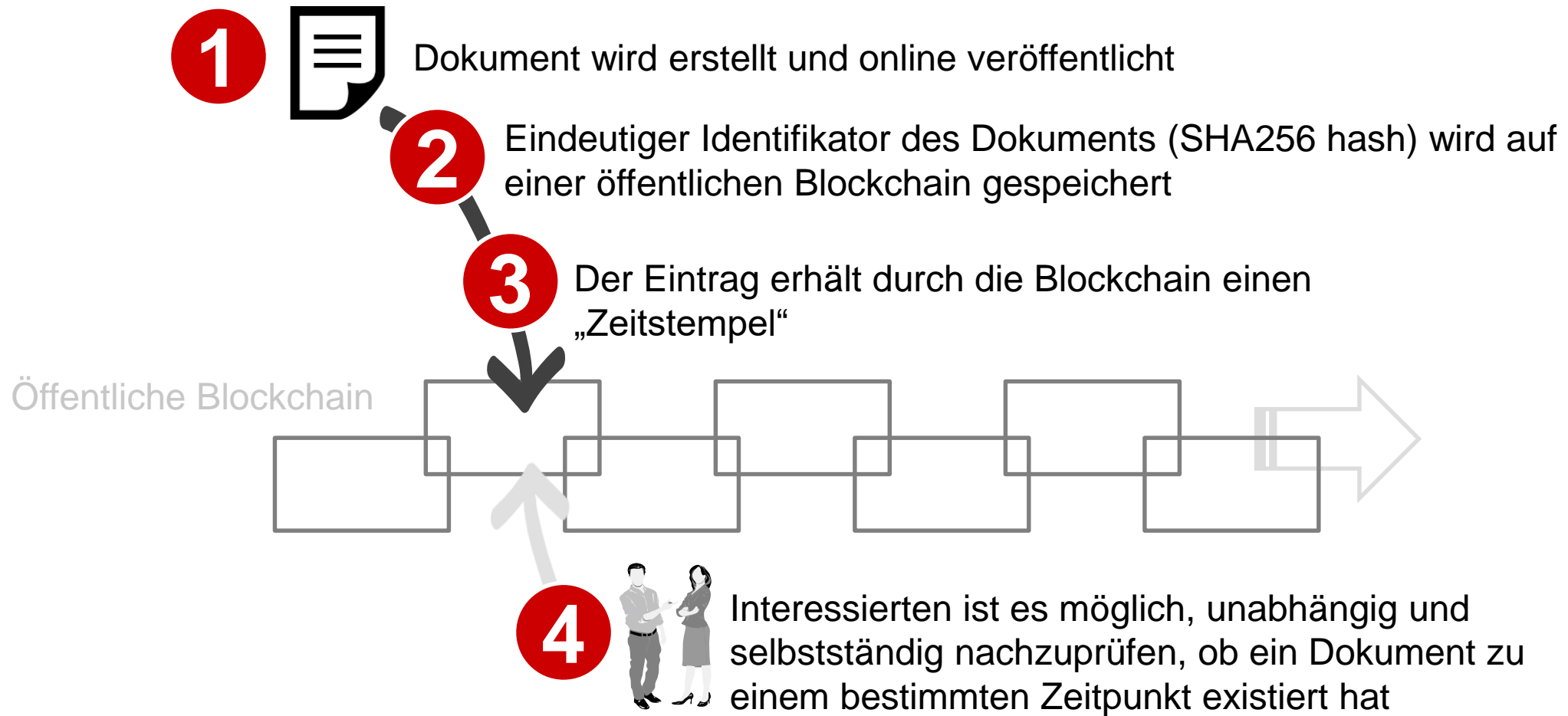
# 1. Blockchain-Pilot der Stadt Wien

## OGD Änderungsprotokoll und Notarisierung

- ❖ Absicherung der Integrität von OGD (Open Government Data) durch Prüfsummen (Hashwerte) in öffentlicher Blockchain
- ❖ Änderungen können nachverfolgt werden
- ❖ Go live: 14.12.2017

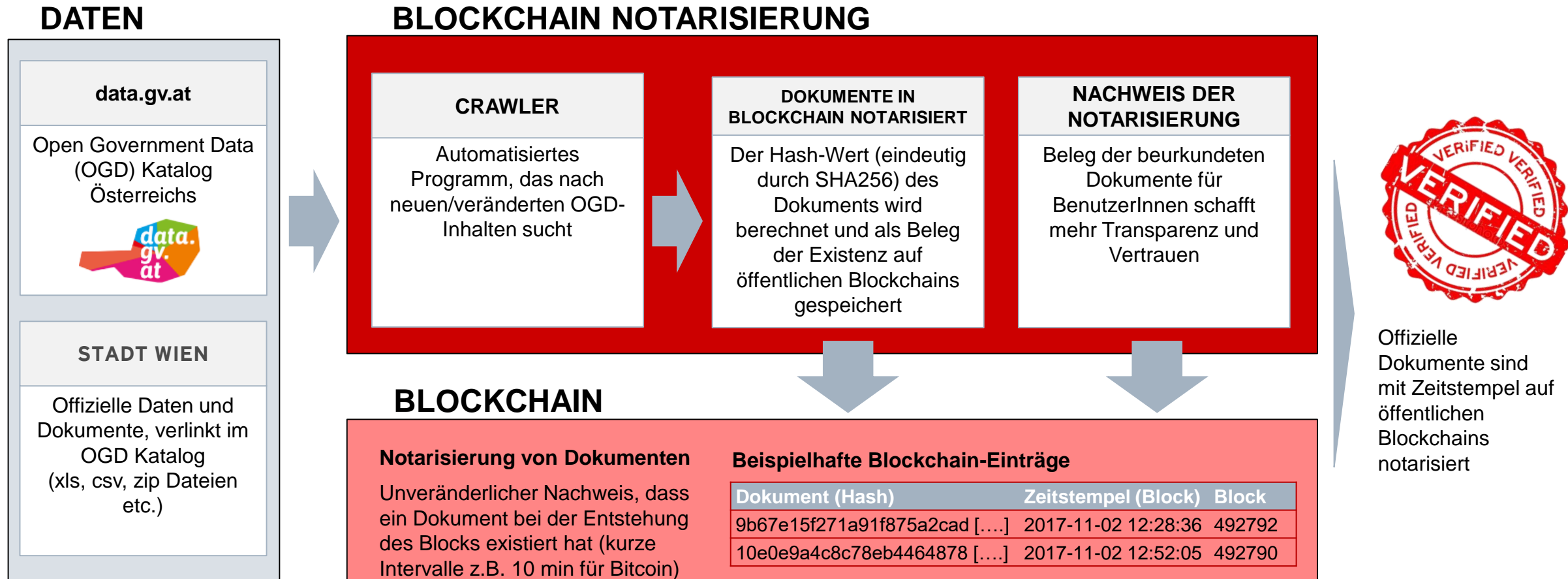


# Die Blockchain ermöglicht nachvollziehbare, öffentliche Nachweise ohne zentrale Autorität



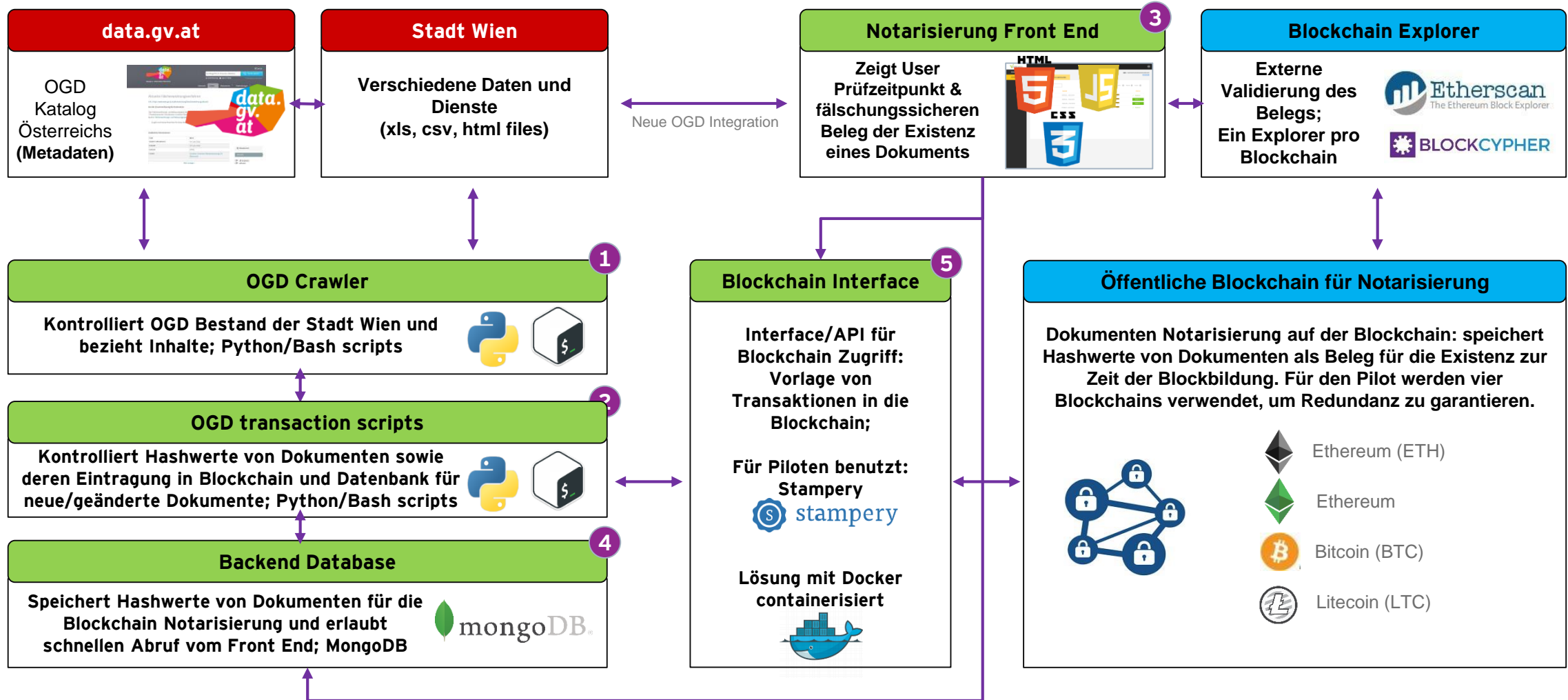
# Stadt Wien Blockchain Pilot: Notarisierung

## Darstellung des Use-Cases



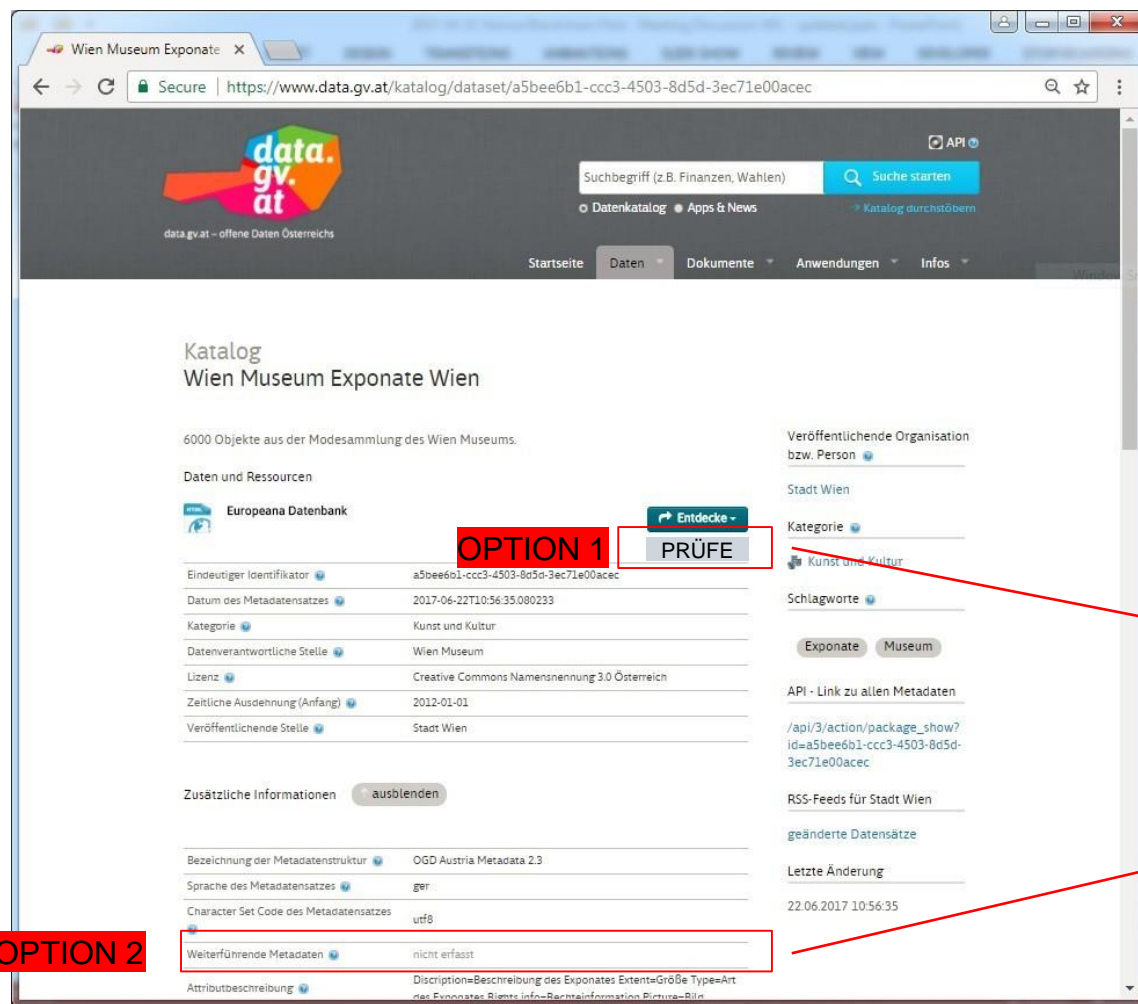
# Stadt Wien Blockchain Pilot: Notarisierung

## Lösungsarchitektur





# Geplante OGD-Integration



## Daten

Vorschlag: Link zum Notarisierung Front-End in das Feld „Weiterführende Metadaten“ speichern – entsprechend OGD Metadaten 2.4

## Interface

Vorschläge zur Integration der Notarisierung in das OGD Webinterface (data.gv.at)

**Option 1:** Wenn Notarisierung verfügbar (Link im Datensatz vorhanden), wird neuer Button „Prüfe Blockchain“ eingefügt

**Option 2:** Link zur Notarisierung Front-End WebApp unter „Weiterführende Metadaten“

# Pilot Screenshots



## Open Government Data - Prüfsummen-Verifizierung

MUSTER

Suchbegriff:

Paketname



add66f20-d033-4eee-b9a0-47019828e698

Suchen

Bitte geben Sie Ihren Suchbegriff ein!

### Impressum

Diese Prüfsummen-Verifizierung ist ein Dienst der Stadt Wien. Es wird keine Gewährleistung für die Richtigkeit der Daten übernommen.

**Verantwortlich für die Seite:**

Magistratsabteilung 14

Automationsunterstützte Datenverarbeitung, Informations- und Kommunikationstechnologie

Stadlauer Straße 56

1220 Wien

E-Mail: [ADV-Web-Redaktion-1@adv.magwien.gv.at](mailto:ADV-Web-Redaktion-1@adv.magwien.gv.at)

StoDt  
Wien

## Open Government Data - Prüfsummen-Verifizierung

Suchbegriff:




Paket	Prüfsumme	Prüfzeitpunkt	URL	Kontakt	Größe	Stampery
add66f20-d033-4eee-b9a0-47019828e698	2e2bef5d530e285e28fcf8a2b2e852fa593c6588e4ab7200f4fd23105e51739d	2017-10-05T15:30:20.0Z	<a href="http://data.wien.gv.at/csv/wienerlinien-ogd-haltestellen.csv">http://data.wien.gv.at/csv/wienerlinien-ogd-haltestellen.csv</a>	<a href="mailto:opendata@wienerlinien.at">opendata@wienerlinien.at</a>	214445	<a href="#">Protokoll</a>
add66f20-d033-4eee-b9a0-47019828e698	2b1cb4d9c3e33ec4a0c90f454acfd65662a0e31b1f4dc563569e345c4abcc66	2017-10-05T15:19:28.0Z	<a href="http://data.wien.gv.at/csv/wienerlinien-ogd-linien.csv">http://data.wien.gv.at/csv/wienerlinien-ogd-linien.csv</a>	<a href="mailto:opendata@wienerlinien.at">opendata@wienerlinien.at</a>	6866	<a href="#">Protokoll</a>
add66f20-d033-4eee-b9a0-47019828e698	d213e82347c1b6996da768adb2a58468a6a515d1eca5a90f995b779b35f49e1	2017-10-05T15:19:28.0Z	<a href="http://data.wien.gv.at/csv/wienerlinien-ogd-steige.csv">http://data.wien.gv.at/csv/wienerlinien-ogd-steige.csv</a>	<a href="mailto:opendata@wienerlinien.at">opendata@wienerlinien.at</a>	659635	<a href="#">Protokoll</a>
add66f20-d033-4eee-b9a0-47019828e698	8d0be379a69b72ad8257625fd8901252a07f60731b7b2adcfe099c96ab53d095	2017-10-05T15:19:28.0Z	<a href="https://go.gv.at/l9ogdwienerlinienteilstreckenwkt">https://go.gv.at/l9ogdwienerlinienteilstreckenwkt</a>	<a href="mailto:opendata@wienerlinien.at">opendata@wienerlinien.at</a>	1219542	<a href="#">Protokoll</a>
add66f20-d033-4eee-b9a0-47019828e698	dbdc22fedfb370c1da5a19a14ce4515c708700700270a8295f1a63d188492f49	2017-10-05T15:19:28.0Z	<a href="https://go.gv.at/l9ogdwienerlinienteilstreckenlonlat">https://go.gv.at/l9ogdwienerlinienteilstreckenlonlat</a>	<a href="mailto:opendata@wienerlinien.at">opendata@wienerlinien.at</a>	2144058	<a href="#">Protokoll</a>

## Impressum

Diese Prüfsummen-Verifizierung ist ein Dienst der Stadt Wien. Es wird keine Gewährleistung für die Richtigkeit der Daten übernommen.

## Verantwortlich für die Seite:

Magistratsabteilung 14

Automationsunterstützte Datenverarbeitung, Informations- und Kommunikationstechnologie

Stadlauer Straße 56

1220 Wien

E-Mail: [ADV-Web-Redaktion-1@adv.magwien.gv.at](mailto:ADV-Web-Redaktion-1@adv.magwien.gv.at)



## Überprüfung der Existenz der Prüfsumme in Blockchains mittels Stampery.com

Mittels dieses Services kann überprüft werden, ob diese Prüfsumme in öffentlichen Blockchains gespeichert wurde. Für technische Details siehe: [stampery.com](https://stampery.com)

Bestätigung von für:

**Paket:** add66f20-d033-4eee-b9a0-47019828e698

**Prüfsumme:** dbdc22fedfb370c1da5a19a14ce4515c708700700270a8295f1a63d188492f49

**Prüfzeitpunkt:** 2017-10-05T15:19:28.0Z

Verifikation in Blockchain:

Prüfung für ltc durchgeführt: "Stampery prüfte erfolgreich!"

Verifizierung in der Blockchain lt mittels eines externen Blockchain-Viewer

Bestätigung von stampery.com:

```
{
  "error": null,
  "result": {
    "time": "2017-10-11 14:08:15.988",
    "token": "798484fc7206b88",
    "receipts": {
      "ltc": {
        "anchors": [
          {
            "sourceId": "7bcc70e0522ba92d80d902effafcc818f32ba368112b1fadce96df42b96977f5",
            "type": "LTCOpReturn",
            "prefix": "53363583",
            "@context": "https://w3id.org/chainpoint/v2",
            "type": "BTA-SHA256",
            "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
            "merkleRoot": "99ACB7549391D7547D7CA5EB8FBC62C8F993E9B0D9FEBCE2EC6528B23EA2B2D39",
            "proof": [
              {
                "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC",
                "right": "9B257F73EC122B80AF3A18485E842CDF98BF1BF5E311EA39E2DB06F8FCD94776",
                "left": "FD932C8080CC6ADCC2FCD7A10BF43B647843F7E55880711D8EFA268E96E83D36"
              }
            ],
            "btc": {
              "anchors": [
                {
                  "sourceId": "4e43f8a2c9612181de791104d4eaab7b2ef10fb5abda92b03ddfbbae5d53ec2b",
                  "type": "BTCOpReturn",
                  "prefix": "53363583",
                  "@context": "https://w3id.org/chainpoint/v2",
                  "type": "BTA-SHA256",
                  "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                  "merkleRoot": "99ACB7549391D7547D7CA5EB8FBC62C8F993E9B0D9FEBCE2EC6528B23EA2B2D39",
                  "proof": [
                    {
                      "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                      "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                      "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                      "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                      "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                      "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                      "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC",
                      "right": "9B257F73EC122B80AF3A18485E842CDF98BF1BF5E311EA39E2DB06F8FCD94776",
                      "left": "FD932C8080CC6ADCC2FCD7A10BF43B647843F7E55880711D8EFA268E96E83D36"
                    }
                  ],
                  "eth": {
                    "anchors": [
                      {
                        "sourceId": "0x70d008fd5712c6f41f7cace07400a24d91c46e423f1ecf0e43889399c1421716",
                        "type": "ETHData",
                        "prefix": "53363583",
                        "@context": "https://w3id.org/chainpoint/v2",
                        "type": "BTA-SHA256",
                        "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                        "merkleRoot": "E62E4DB0DF9D3E6BC273C7E7DDE3C06085FF226AFD8EAC38DE30A38AB174B3B5",
                        "proof": [
                          {
                            "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                            "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                            "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                            "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                            "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                            "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                            "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC",
                            "right": "9B257F73EC122B80AF3A18485E842CDF98BF1BF5E311EA39E2DB06F8FCD94776",
                            "left": "FD932C8080CC6ADCC2FCD7A10BF43B647843F7E55880711D8EFA268E96E83D36"
                          }
                        ],
                        "etc": {
                          "anchors": [
                            {
                              "sourceId": "0x0f77de9a6ebf0fe10971aa93e37dfb3ecf4d233c6245b089b28e4591ed2dda92",
                              "type": "ETCData",
                              "prefix": "53363583",
                              "@context": "https://w3id.org/chainpoint/v2",
                              "type": "BTA-SHA256",
                              "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                              "merkleRoot": "E62E4DB0DF9D3E6BC273C7E7DDE3C06085FF226AFD8EAC38DE30A38AB174B3B5",
                              "proof": [
                                {
                                  "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                                  "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                                  "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                                  "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                                  "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                                  "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                                  "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC",
                                  "right": "9B257F73EC122B80AF3A18485E842CDF98BF1BF5E311EA39E2DB06F8FCD94776",
                                  "left": "FD932C8080CC6ADCC2FCD7A10BF43B647843F7E55880711D8EFA268E96E83D36"
                                }
                              ],
                              "hash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                              "id": "59de25cf4b1b9d0004b4856e"
                            }
                          ]
                        }
                      }
                    ]
                  }
                }
              ]
            }
          }
        ]
      }
    }
  }
}
```

## Impressum

Diese Prüfsummen-Verifizierung ist ein Dienst der Stadt Wien. Es wird keine Gewährleistung für die Richtigkeit der Daten übernommen.

Verantwortlich für die Seite:

Magistratsabteilung 14

Automationsunterstützte Datenverarbeitung, Informations- und Kommunikationstechnologie

Stadlauer Straße 56

1220 Wien

E-Mail: [ADV-Web-Redaktion-l@adv.magwien.gv.at](mailto:ADV-Web-Redaktion-l@adv.magwien.gv.at)

# Beispiel für externe Validierung in Blockchain Explorer „Blockcypher“

The screenshot shows the Blockcypher website interface for a Bitcoin transaction. The transaction ID is highlighted with a red box. Below it, a warning message about embedded data is also highlighted. At the bottom, a summary bar shows transaction details, with the 'RECEIVED' timestamp highlighted by a red box. A red arrow points from the timestamp box to the label 'Timestamp des Blocks' on the right.

**Transaction ID:** 4e43f6a2c9612181de791104d4eaab7b2ef10fb5abda92b03ddfbbae5d53ec2b

**Warning:** Data Embedded in Transaction with Unknown Protocol (what's this?)  
Hex: 5336358b99acb7549391d7547d7ca5eb8fbc62c8f993e9b0d9feb2ec6528b23ea2b2d39

**Transaction Summary:**

AMOUNT TRANSACTED	FEES	RECEIVED	CONFIRMATIONS
0.08006523 BTC	0.00015 BTC	🕒 26 days ago 2017-10-11 14:34 GMT	🔒 6+

Advanced Details ▾

Details

Transaktions-ID

Merkle-Root (und Prefix)

Timestamp des Blocks

# Digitalisierung, Daten und Open Innovation

## Wir schaffen Mehrwert

---

Mag.<sup>a</sup> Ulrike Huemer

[ulrike.huemer@wien.gv.at](mailto:ulrike.huemer@wien.gv.at)

Ing.<sup>in</sup> Brigitte Lutz, MSc

[brigitte.lutz@wien.gv.at](mailto:brigitte.lutz@wien.gv.at)

Bernd Wünschek

[bernd.wuenschek@wien.gv.at](mailto:bernd.wuenschek@wien.gv.at)

Open Government - Kompetenzzentrum Wien

[open@post.wien.gv.at](mailto:open@post.wien.gv.at)

[open.wien.gv.at](http://open.wien.gv.at)



Diese Präsentation der Stadt Wien steht unter einer [Creative Commons Namensnennung 3.0 Österreich Lizenz](https://creativecommons.org/licenses/by/3.0/).

Die Namensnennung der Stadt Wien als Rechteinhaberin hat in folgender Weise zu erfolgen:

"Datenquelle: Stadt Wien"

# Appendix

---



# Beschreibung der verwendeten Module

1 OGD Crawler	2 OGD transaction scripts	3 Notarisierung Front End	4 Backend Database	5 Blockchain Interface
<p>OGD Crawler-Script kontrolliert data.gv.at auf neue/veränderte Daten der Stadt Wien</p> <ul style="list-style-type: none"> <li>▶ Neue Daten → Hashwert wird generiert und in DB geschrieben</li> <li>▶ Existierende Daten → Hashwert wird generiert und mit gespeichertem verglichen</li> <li>▶ Wenn Hashwerte ident, keine Aktion</li> <li>▶ Wenn neuer Hashwert anders &amp; stabil (3x geprüft) → in DB geschrieben</li> </ul> <p>Aktuell nur Stadt Wien-Inhalte. GIS und Echtzeitdaten derzeit nicht.</p>	<p>Script kontrolliert auf neue oder aktualisierte Daten</p> <ul style="list-style-type: none"> <li>▶ Neu oder aktualisiert: sendet Transaktion mit neuem Hashwert an</li> <li>▶ Option 1: Drittanbieter z.B. stampery</li> <li>▶ Option 2: Eigene API &amp; Smart Contract</li> <li>▶ Neu: schickt URL zu data.gv.at (Metadaten) → Zugang zu Notarisierung Front End</li> <li>▶ Schreibt Info in DB (Transaktion j/n Flagge, URL)</li> </ul>	<ul style="list-style-type: none"> <li>▶ Auf das Notarisierung Front End kann via URL in den Metadaten auf data.gv.at zugegriffen werden</li> <li>▶ Vom Front End kann auf einen Blockchain Explorer zugegriffen werden</li> </ul>	<ul style="list-style-type: none"> <li>▶ Speichert Hashwerte von Dokumenten für den Vergleich zwischen verschiedenen Crawl Runs</li> <li>▶ Speichert Werte für schnellen Abruf vom Front End</li> <li>▶ Jede Information kann durch echte Blockchain Einträge nachgeprüft werden</li> </ul>	<p>Option 1: Service von Drittanbieter z.B. Stampery:</p> <ul style="list-style-type: none"> <li>• Vorteil: schnellere Entwicklung,</li> <li>• Nachteil: abhängig von Drittanbieter, weniger flexibel</li> </ul> <p>Option 2: Entwicklung eigener API:</p> <ul style="list-style-type: none"> <li>• Vorteil: Flexibilität, Unabhängigkeit</li> <li>• Nachteil: Entwicklungs-Aufwand</li> </ul> <p>Smart Contract</p> <p>Option 1: Bei Drittanbieter nicht notwendig.</p> <p>Option 2: Bei eigener API ist Smart Contract notwendig. Sollte so einfach und kurz wie möglich sein.</p>



## Überprüfung der Existenz der Prüfsumme in Blockchains mittels Stampery.com

Mittels dieses Services kann überprüft werden, ob diese Prüfsumme in öffentlichen Blockchains gespeichert wurde. Für technische Details siehe: [stampery.com](https://stampery.com)

Bestätigung von für:

**Paket:** add66f20-d033-4eee-b9a0-47019828e698  
**Prüfsumme:** dbdc22fedfb370c1da5a19a14ce4515c708700700270a8295f1a63d188492f49  
**Prüfzeitpunkt:** 2017-10-05T15:19:28.0Z

Verifikation in Blockchain:

keine Prüfung gestartet

[Verifizierung in der Blockchain ltc mittels eines externen Blockchain-Viewer](#)

Bestätigung von stampery.com:

```
{
  "error": null,
  "result": {
    "time": "2017-10-11 14:08:15.988",
    "token": "798484fc7206b88",
    "receipts": {
      "ltc": {
        "anchors": [
          {
            "sourceId": "7bcc70e0522ba92d80d902effafcc818f32ba368112b1fadce96df42b96977f5",
            "type": "LTCOpReturn",
            "prefix": "53363583",
            "@context": "https://w3id.org/chainpoint/v2",
            "type": "BTA-SHA256",
            "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
            "merkleRoot": "99ACB7549391D7547D7CA5EB8FBC62C8F993E9B0D9FEBEC2EC6528B23EA2B2D39",
            "proof": [
              {
                "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC",
                "right": "9B257F73EC122B80AF3A18485E842CDF98BF1BF5E311EA39E2DB06F8FCD94776",
                "left": "FD932C8080CC6ADCC2FCD7A10BF43B647843F7E55880711D8EFA268E96E83D36"
              ]
            ],
            "btc": {
              "anchors": [
                {
                  "sourceId": "4e43f6a2c9612181de791104d4eaab7b2ef10fb5abda92b03ddfbbae5d53ec2b",
                  "type": "BTCOpReturn",
                  "prefix": "53363583",
                  "@context": "https://w3id.org/chainpoint/v2",
                  "type": "BTA-SHA256",
                  "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                  "merkleRoot": "99ACB7549391D7547D7CA5EB8FBC62C8F993E9B0D9FEBEC2EC6528B23EA2B2D39",
                  "proof": [
                    {
                      "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                      "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                      "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                      "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                      "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                      "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                      "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC",
                      "right": "9B257F73EC122B80AF3A18485E842CDF98BF1BF5E311EA39E2DB06F8FCD94776",
                      "left": "FD932C8080CC6ADCC2FCD7A10BF43B647843F7E55880711D8EFA268E96E83D36"
                    ]
                  ],
                  "eth": {
                    "anchors": [
                      {
                        "sourceId": "0x70d008fd5712c6f41f7cace07400a24d91c46e423f1ecf0e43889399c1421716",
                        "type": "ETHData",
                        "prefix": "53363583",
                        "@context": "https://w3id.org/chainpoint/v2",
                        "type": "BTA-SHA256",
                        "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                        "merkleRoot": "E62E4DB0DF9D3E6BC273C7E7DDE3C06085FF226AFD8EAC38DE30A38AB174B3B5",
                        "proof": [
                          {
                            "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                            "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                            "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                            "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                            "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                            "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                            "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC"
                          ]
                        ],
                        "etc": {
                          "anchors": [
                            {
                              "sourceId": "0x0f77de9a6ebf0fe10971aa93e37dfb3ecf4f233c6245b089b28e4591ed2dda92",
                              "type": "ETCData",
                              "prefix": "53363583",
                              "@context": "https://w3id.org/chainpoint/v2",
                              "type": "BTA-SHA256",
                              "targetHash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                              "merkleRoot": "E62E4DB0DF9D3E6BC273C7E7DDE3C06085FF226AFD8EAC38DE30A38AB174B3B5",
                              "proof": [
                                {
                                  "right": "58A563F63A40EC0901B79A3358B4822B0B2E6868BFD8F6FE97FBD478F688C81",
                                  "right": "B55FE9DAF3EE5C1E5601FA3D675CC846D545B43AAB3C3D94273CDC57B8C43B6F",
                                  "right": "ED26148A44BAE509DE50E994D4E05CE3B77DE9E0B467ED3DCE81392B8F5ADB01",
                                  "right": "BB1352193972A75E7D44DF315D48963F4AD1766F73CAD287DE29F1601FF80D57",
                                  "right": "42299E1AAE275E94360639E37685D907247C772842318ECA9F3FA56BA29D5DD3",
                                  "right": "42EAB3B613C9C02749F44197E4A4C68DF9F43BA79B74966B06A2C843B5029EE1",
                                  "right": "42EB5452E34B126DEC7751B77357EB4FBDB9B15DE7EF665512CC110739A1B9EC"
                                ]
                              ],
                              "hash": "DBDC22FEDFB370C1DA5A19A14CE4515C708700700270A8295F1A63D188492F49",
                              "id": "59de25cf4b1b9d0004b4856e"
                            ]
                          ]
                        }
                      ]
                    ]
                  ]
                }
              ]
            ]
          }
        ]
      }
    }
  }
}
```

## Impressum

Diese Prüfsummen-Verifizierung ist ein Dienst der Stadt Wien. Es wird keine Gewährleistung für die Richtigkeit der Daten übernommen.

Verantwortlich für die Seite:

Magistratsabteilung 14

Automationsunterstützte Datenverarbeitung, Informations- und Kommunikationstechnologie

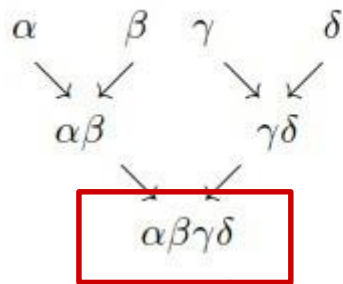
Stadlauer Straße 56

1220 Wien

E-Mail: [ADV-Web-Redaktion-l@adv.magwien.gv.at](mailto:ADV-Web-Redaktion-l@adv.magwien.gv.at)

# Funktionsweise des Blockchain Interface

## Merkle Tree



**Figure 1:** Example of Merkle tree with 4 hashes as leaf nodes.

- Merkle Path wird für Beweisfunktion gespeichert.
- Externes Service (Stampery) für Pilot
- Dieses Service intern realisieren?

Öffentliche Blockchain

