# Open Goverment Data der Stadt Wien in Blockchain prüfen

## Schritt-für-Schritt-Anleitung

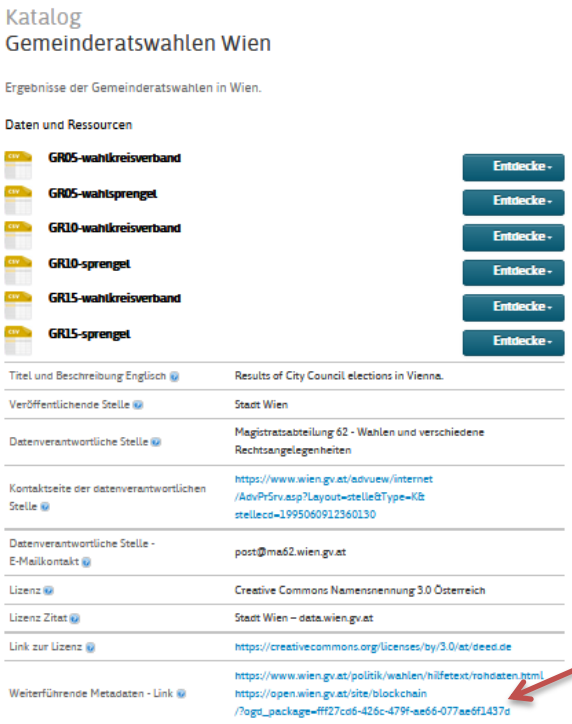
In einem ersten Piloten ermöglicht die Stadt Wien, dass die interessierte Öffentlichkeit die Richtigkeit von Open Government Data (OGD) mittels Blockchain-Technologie überprüfen kann. Die Anwendung wird nachfolgend anhand des Beispiels "Wiener Ergebnis der Gemeinderatswahl" Schritt für Schritt erklärt.

### 1. Öffentliche Daten finden

Unter open.wien.gv.at bzw. https://www.data.gv.at im Suchfeld beispielsweise „Gemeinderatswahlen Wien“ eingeben.

Das ausgeworfene Suchergebnis zeigt, dass es für die Gemeinderatswahlen 2005, 2010 und 2015 Daten gibt.

### 2. Prüfservice aufrufen



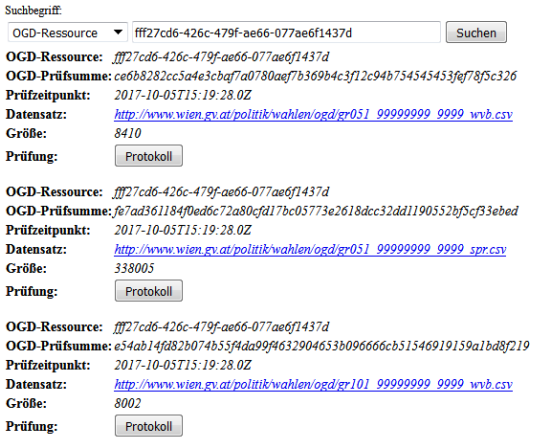

In den weiterführenden Metadaten ist der Link zum Prüfservice „Open Data in Blockchain prüfen“ enthalten:

https://open.wien.gv.at/site/blockchain/?ogd_package=fff27cd6-426c-479f-ae66-077ae6f1437d

Dabei ist "fff27cd6-426c-479f-ae66-077ae6f1437d" die eindeutige Bezeichnung für die Daten der OGD-Ressource.

## 3. Änderungsprotokoll

Durch den Klick auf den Link in den weiterführenden Metadaten öffnet sich eine Seite mit dem Änderungsprotokoll.




Die OGD-Ressource ist bereits ausgefüllt. Es ist aber auch jederzeit möglich, im Prüfservice andere OGD-Ressourcen zu prüfen oder eine OGD-Prüfsumme als Suchbegriff zu verwenden, um die Korrektheit eines Datenbestandes zu überprüfen.

Zum jeweiligen Datensatz (in diesem Falle die csv-Datei), werden einige Informationen angezeigt, wie die OGD-Prüfsumme und der genaue Zeitpunkt, wann die jeweilige Ressource vorhanden war.

## 4. Blockchain prüfen

Mit dem Klick auf "Protokoll" gelangen Sie zum Kernstück des Prüfservices: den in der Blockchain verankerten Daten.


Derzeit werden vier Blockchains benutzt, um hier von technischen Entwicklungen möglichst unabhängig zu sein:

- LTC Litecoin
- BTC Bitcoin
- ETH Ethereum
- ETC Ethereum Classic

Diese Blockchains enthalten Buchungen in den jeweiligen Kryptowährungen.

Dazu wird im Pilotprojekt der Stadt Wien die Technologie des *Blockchain*-Unternehmens *Stampery* https://www.stampery.com genutzt, das die Dokumentenzertifizierung auf Grundlage der o.a. Blockchains bietet.

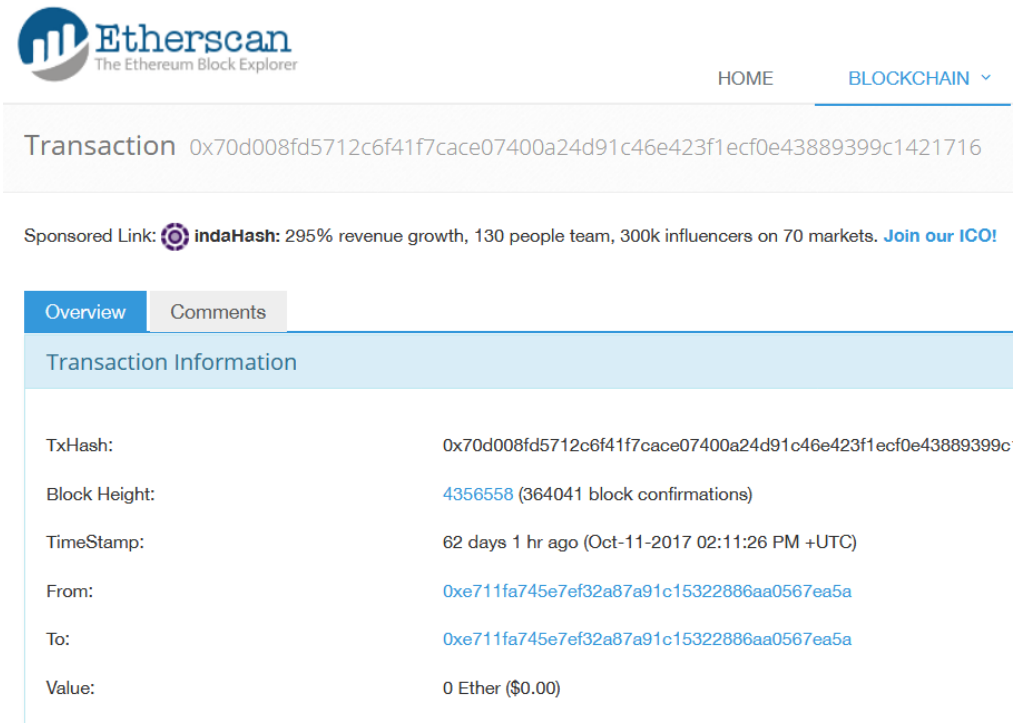
Im "Betreff" einer Buchung wird der Beweis abgelegt, dass zu einem bestimmten Zeitpunkt (als der aktuelle "Block" der Buchungen erzeugt wurde) die oben gefundene SHA256-Prüfsumme existiert hat.

Der "Prüfzeitpunkt" ist jener Zeitpunkt, an dem der Datenbestand in dieser Form das erste Mal überprüft wurde. Dabei wurde die SHA256-Prüfsumme festgestellt, das ist eine (lange) Zahl, bei deren Berechnung kryptografisch sichergestellt wird, dass unterschiedliche Daten auch unterschiedliche Prüfsummen haben,
z.B. "fe7ad361184f0ed6c72a80cfd17bc05773e2618dcc32dd1190552bf5cf33ebed“.

Technische Details zu "kryptografischen Hashes" sind z.B. unter https://de.wikipedia.org/wiki/SHA-2 nachzulesen.

Wählen Sie die Blockchain aus, für die die Prüfung ausgeführt werden soll. Wenn Sie auf „Prüfen“ klicken, wird die Prüfung über das Webservice von Stampery durchgeführt.

Zusätzlich können Sie in der jeweiligen Blockchain mittels eines externen Blockchain-Viewers den jeweiligen Eintrag in der Blockchain verifizieren:
z.B. Verifizierung in der Blockchain Ethereum mittels eines externen Blockchain-Viewer




Diese Funktion ist von der Stadt Wien vollständig unabhängig.

## Zusätzliche Überprüfung des sicheren Hash-Algorithmus

Misstrauen Sie der Überprüfungs-Funktion von Stampery, ist es möglich, den "Beweis", der unter dem Punkt "Protokoll" abrufbar ist, selbst vollständig nachzuvollziehen, das ist allerdings mit technischem Aufwand verbunden. In der Dokumentation von Stampery.com ist die Vorgangsweise beschrieben: Unter https://stampery.com/tech ist das "Whitepaper" verfügbar, das die Technik detailliert genug beschreibt, um sie unabhängig nachzuprüfen.

Wenn Sie selbst nachprüfen möchten, ob die aktuellen Daten die angegebene SHA256-Prüfsumme ergeben, holen Sie sich die OGD-Daten auf den Computer (zum Beispiel durch Anklicken der URL https://www.wien.gv.at/politik/wahlen/ogd/gr151_99999999_9999_spr.csv) und können diese SHA256-Prüfsumme selbst berechnen und mit der Behauptung auf der Webseite vergleichen, z.B. mit dem Programm "7zip" (http://www.7-zip.org/) - hier gibt es diese praktische Funktion im Kontext-Menü (mit der rechten Maustaste über der Datei).

Dadurch ist eine Überprüfung unabhängig von "Stampery" und unabhängig von der Stadt Wien möglich. Der Weg von der Prüfsumme der OGD-Ressource zu dem Hashwert in der Blockchain („Merkle-Root“) ist im „Beweis“ enthalten, dieser sogenannten „Merkle-Path“ erlaubt eine nicht fälschbare, schrittweise Überprüfung der Kette der Hashwerte.