

Open Government 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

Katalog
Gemeinderatswahlen Wien

Ergebnisse der Gemeinderatswahlen in Wien.

Daten und Ressourcen

 GR05-wahlkreisverband	Entdecke -
 GR05-wahlsprengel	Entdecke -
 GR10-wahlkreisverband	Entdecke -
 GR10-sprengel	Entdecke -
 GR15-wahlkreisverband	Entdecke -
 GR15-sprengel	Entdecke -

Titel und Beschreibung Englisch	Results of City Council elections in Vienna.
Veröffentlichende Stelle	Stadt Wien
Datenverantwortliche Stelle	Magistratsabteilung 62 - Wahlen und verschiedene Rechtsangelegenheiten
Kontaktseite der datenverantwortlichen Stelle	https://www.wien.gv.at/advview/internet/AdvPrSrv.asp?Layout=stelle&Type=K&stellecd=1995060912360130
Datenverantwortliche Stelle - E-Mailkontakt	post@ma62.wien.gv.at
Lizenz	Creative Commons Namensnennung 3.0 Österreich
Lizenz Zitat	Stadt Wien – data.wien.gv.at
Link zur Lizenz	https://creativecommons.org/licenses/by/3.0/at/deed.de
Weiterführende Metadaten - Link	https://www.wien.gv.at/politik/wahlen/hilfetext/rohdaten.html https://open.wien.gv.at/site/blockchain/?ogd_package=fff27cd6-426c-479f-ae66-077ae6f1437d

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.

Suchbegriff:
OGD-Ressource:

OGD-Ressource: [fff27cd6-426c-479f-ae66-077ae6f1437d](#)
OGD-Prüfsumme: [ce6b8282cc5a4e3cbaf7a0780aef7b369b4c3f12c94b754545453fef78f5c326](#)
Prüfzeitpunkt: 2017-10-05T15:19:28.0Z
Datensatz: http://www.wien.gv.at/politik/wahlen/ogd/gr051_99999999_9999_wvb.csv
Größe: 8410
Prüfung:

OGD-Ressource: [fff27cd6-426c-479f-ae66-077ae6f1437d](#)
OGD-Prüfsumme: [fe7ad361184f0ad6c72a80cf17bc05773e2618dec32dd1190552bf5cf33ebed](#)
Prüfzeitpunkt: 2017-10-05T15:19:28.0Z
Datensatz: http://www.wien.gv.at/politik/wahlen/ogd/gr051_99999999_9999_spr.csv
Größe: 338005
Prüfung:

OGD-Ressource: [fff27cd6-426c-479f-ae66-077ae6f1437d](#)
OGD-Prüfsumme: [e54ab14fd82b074b55f4da99f4632904653b096666cb51546919159a1ba8f219](#)
Prüfzeitpunkt: 2017-10-05T15:19:28.0Z
Datensatz: http://www.wien.gv.at/politik/wahlen/ogd/gr101_99999999_9999_wvb.csv
Größe: 8002
Prüfung:

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.

Bestätigung für:

OGD-Ressource: [fff27cd6-426c-479f-ae66-077ae6f1437d](#)
OGD-Prüfsumme: [ce6b8282cc5a4e3cbaf7a0780aef7b369b4c3f12c94b754545453fef78f5c326](#)
Prüfzeitpunkt: 2017-10-05T15:19:28.0Z

Verifikation in Blockchain:

Prüfung für Ethereum Classic durchgeführt: "Stampery prüfte erfolgreich!"

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

Bestätigung von stampery.com:

```
{  
  "error": null,  
  "result": [  
    ]  
}
```

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,

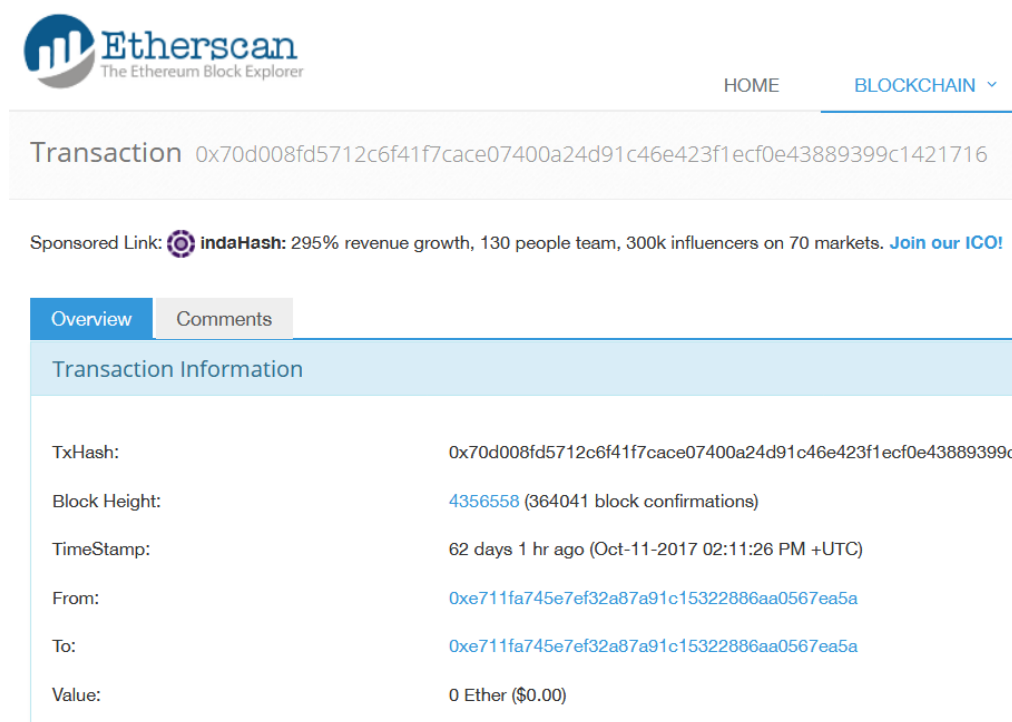
z.B. "fe7ad361184f0ed6c72a80cfd17bc05773e2618dcc32dd1190552bf5cf33ebed".

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](#)



The screenshot shows the Etherscan interface for a specific transaction. At the top left is the Etherscan logo with the tagline "The Ethereum Block Explorer". To the right are navigation links for "HOME" and "BLOCKCHAIN". The main header displays "Transaction" followed by the transaction hash: 0x70d008fd5712c6f41f7cace07400a24d91c46e423f1ecf0e43889399c1421716. Below this is a sponsored link for "indaHash" with details: "295% revenue growth, 130 people team, 300k influencers on 70 markets. Join our ICO!". The transaction details are presented in a table with two tabs: "Overview" (selected) and "Comments". The table lists the following information:

Transaction Information	
TxHash:	0x70d008fd5712c6f41f7cace07400a24d91c46e423f1ecf0e43889399c
Block Height:	4356558 (364041 block confirmations)
TimeStamp:	62 days 1 hr ago (Oct-11-2017 02:11:26 PM +UTC)
From:	0xe711fa745e7ef32a87a91c15322886aa0567ea5a
To:	0xe711fa745e7ef32a87a91c15322886aa0567ea5a
Value:	0 Ether (\$0.00)

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.