

Privatgutachterliche Stellungnahme

**Daten-Zertifizierung
auf Basis Blockchain**



erstellt von

Mag. Dipl-Ing. Dr. Markus Knasmüller
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger

im Auftrag von

AUSTRIAPRO
Wiedner Hauptstraße 63
A – 1045 Wien

Haag, Dezember 2019

Gegenstand des Gutachtens

Erstellung einer privatgutachterlichen Stellungnahme, in der die „Daten Zertifizierung“ auf Basis Blockchain behandelt wird. Folgende Themen sind dabei vorgesehen:

- Beschreibung System und Funktionsweise (Beispiel siehe: <https://blockchains.web-lab.at/docnos/>)
- Verwendete Technologien & Standards
 - Multichain; Opensource ...
 - Hashwertberechnungen lt. mindestens SHA-2/256 oder SHA-3
- Praktische Versuche (z.B. im Rahmen des AUSTRIAPRO Blockchain Labs)

Zur Person des Sachverständigen

Dr. Markus Knasmüller ist seit 2003 allgemein beeideter und gerichtlich zertifizierter Sachverständiger (eingetragen am Landesgericht Steyr) und u.a. für folgende Bereiche zertifiziert:

- **Informationstechnik** - Softwaretechnik, Programmierung
- **Informationstechnik** - Internetsoftware, WEB Programmierung, Netzwerkanwendung
- **Informationstechnik** - Anwendungssoftware, Standardprogramme
- **Informationstechnik** – IT Sicherheit, Datenschutz, Verschlüsselung und Signaturerstellung, Virenschutz

Dr. Knasmüller ist außerdem als Leiter der Fachgruppe Informations- und Kommunikationstechnik Vorstandsmitglied des Hauptverbandes der Gerichtssachverständigen, Landesverband Oberösterreich und Salzburg und er ist auch Leiter des Arbeitskreises Kassensoftware beim Fachverband UBIT der Wirtschaftskammer Österreich.

Einleitung

Gegenstand dieser privatgutachterlichen Stellungnahme ist das Blockchain-Service Datenzertifizierung der Wirtschaftskammer Österreich (WKO). Mit diesem Service (www.wko.at/service/innovation-technologie-digitalisierung/blockchain.html) lassen sich Daten einfach, sicher und kostenlos digital zertifizieren. Unabhängig vom Datenformat erhalten Daten dabei einen Zeitnachweis, wann sie entstanden sind, vorgelegt oder verändert wurden.

Folgende Themen wurden dabei mit dem Auftraggeber AUSTRIAPRO vereinbart:

- Beschreibung System und Funktionsweise (Beispiel siehe: <https://blockchains.web-lab.at/docnos/>)
- Verwendete Technologien & Standards
 - Multichain; Opensource ...
 - Hashwertberechnungen lt. mindestens SHA-2/256 oder SHA-3
- Praktische Versuche (zB im Rahmen des AUSTRIAPRO Blockchain Labs)

Das Gutachten ist dementsprechend auch in diese Abschnitte aufgeteilt, wobei eine abschließende Stellungnahme in der Zusammenfassung enthalten ist.

In dieser Einführung erscheint es dem Sachverständigen aber auch wesentlich einerseits den Arbeitskreis Blockchain von AUSTRIAPRO, wie auch einige Grundlagen zum Thema Blockchain zu präsentieren.

Der Arbeitskreis Blockchain von AUSTRIAPRO¹ wurde 2018 gegründet mit folgenden Zielen:

- Information (z.B. bei welchen Geschäftsprozessen ist die Blockchain sinnvoll?)
- Diskussion (Einsatzgebiete, Chancen, Risiken, nationale und internationale Entwicklungen)
- Testbed (Labs) für gefahrloses Ausprobieren von Blockchain Anwendungen
- Pilotprojekte (welche effizienten und sicheren Einsatz der Blockchain Technologie vorzeigen)
- Erarbeitung von Standards, wo nötig

Folgende Punkte wurden dabei als Nicht-Ziele definiert:

- Blockchain allgemein „promoten“
- einzelne Lösungen favorisieren
- das Thema Kryptowährungen

Die folgenden Definitionen zum Thema Blockchain sind dem Buch von Niklas Schmidt, *Kryptowährungen und Blockchains*, Linde (2019), entnommen und sollten einem nicht so versierten Leser einige Grundlagen näherbringen.

Eine **Blockchain** ist eine Kette aus Blöcken, wobei jeder einzelne Block wiederum Transaktionen enthält. Somit ist eine Blockchain im Grunde eine Liste von Transaktionen bzw. in der Sprache der Buchhaltung ein Journal. Die Blöcke werden mithilfe eines mathematischen (kryptografischen) Verfahrens miteinander verkettet.

¹ www.wko.at/service/netzwerke/austriapro-arbeitskreis-blockchain.html

Ein **Block** sind dabei mehrere Transaktionen von Bitcoins (oder aber auch andere zu speichernde Daten), die aus administrativen Gründen zusammengefasst werden. Ein Block ist also ein Container in dem mehrere Transaktionen gespeichert sind.

Eine **Transaktion** ist grundsätzlich die Übertragung von Bitcoins von einer Adresse an eine andere Adresse. Allerdings können im Journal alle möglichen Arten von Transaktionen verzeichnet werden und zwar auch betreffend körperlicher und unkörperlicher Wirtschaftsgüter.

Wesentlich ist, dass man sich die Blockchain vorstellen kann, wie ein Buch. Alle Seiten können weder entfernt noch geändert werden. Das Buch wird also immer nur dicker. Auf den einzelnen Seiten sind Transaktionen dargestellt.

Dabei gibt es nicht nur eine einzige Kopie der Blockchain, sondern **Kopien** dieser Transaktionsdatenbank auf einem Peer-to-Peer-Netzwerk von unabhängigen Rechnern. Jeder kann in die Blockchain Einsicht nehmen. Wenn man eine an der Transaktion beteiligte Adresse oder die Identifikationsnummer der Transaktion kennt, kann man diese in einen Block Explorer eingeben um weitere Informationen zu erhalten.

Der **Konsensmechanismus** soll sicherstellen, dass nur Blöcke mit korrekten Transaktionen angefügt werden. Es gibt mehrere Mechanismen, diesen Konsens zu ermitteln:

- Proof of Work: Hier werden Transaktionen von Personen abgezeichnet, die beweisen („proof“) können, Arbeit („work“) eingesetzt zu haben.
- Proof of Stake: Hier werden Transaktionen von Personen abgezeichnet, die hohe Bestände an einer bestimmten Kryptowährung halten.
- Multi Signature: Hier müssen z.B. drei von fünf Teilnehmern des Netzwerks Transaktionen abzeichnen.

Auch wenn klassisch in der Blockchain Kryptowährungen, wie Bitcoin, gespeichert werden, so ist dies nicht die einzige Anwendungsart. Unter Tokenisierung versteht man demnach, dass Güter wie z.B. Grundstücke, Aktien, Forderungen, Genussrechte oder Goldbarren durch auf einer Blockchain verzeichnete Tokens repräsentiert werden.

Ein Anwendungsbeispiel, sind dabei auch **Smart Contracts**, die in der Ethereum-Plattform gespeichert werden. Bei **Etherum** handelt es sich um eine auf der Blockchain-Technologie von Bitcoin basierende Plattform. Statt Bitcoins auf der Blockchain zu speichern, werden aber dort Programme (sogenannte Smart Contracts) gespeichert.

Smart Contracts sind Programme (meist bestehend aus einfachen Wenn-dann-Anweisungen), die auf der Blockchain gespeichert sind, nicht geändert werden können, vollautomatisch ablaufen (d.h. ohne Störungsmöglichkeiten durch die Parteien oder durch Dritte) und über auf der Blockchain gespeicherte Wirtschaftsgüter verfügen können. Diese sind zivilrechtlich gültig – obwohl sie gänzlich in Programmcode verfasst sind. Eine Willenserklärung kann auch durch Verwendung einer Programmiersprache ausgedrückt werden, sofern der Erklärende selbst den Inhalt seiner Willenserklärung versteht.

Beispiele für Smart Contracts:

- Crowdfunding: Wenn bis zu einem bestimmten Datum ein definierter Betrag an dieser Adresse eingelangt ist, wird er an den Projektbetreiber weitergeleitet und dieser startet das Projekt, anderenfalls bekommen die Investoren ihr Geld zurücküberwiesen.
- Ein Smart Contract kann auch als Testamentersatz Anwendung finden. Wenn eine bestimmte Person stirbt, könnte z.B. vorgesehen werden, dass ein Eintrag in einer auf Blockchain-Basis geführten Grundstücksdatenbank auf einen Erben umgeschrieben wird.
- KFZ-Registrierung
- Automatisches Reagieren auf Zahlungsverzug indem z.B. ein Auto nicht weiterfährt

Technisch basieren Blockchains auf kryptographische Hashes. Ein **kryptographischer Hash** ist ein eindeutiger digitaler Fingerabdruck eines bestimmten Inhalts, eine Art Prüfsumme. Es handelt sich dabei um eine Einwegfunktion, die man sich wie einen Fleischwolf vorstellen kann. Füttert man in die Funktion einen bestimmten Inhalt, so erhält man eine Zeichenkette (Hash) mit immer gleicher Länge (eine Binärzahl mit 256 Stellen) als Ergebnis. Jede noch so geringe Veränderung des Inputs führt zu einem komplett anderen – nicht vorhersehbaren – Output. Es ist praktisch unmöglich, von einem Hash auf den dazugehörigen Input rückzuschließen.

Hashwerte kommen etwas auch bei der Sicherung der Integrität der verwendeten Software in Glückspielautomaten vor (vgl. § 24 Automatenglückspielverordnung) oder bei der Verschlüsselung der Umsatzzähler bei Registrierkassen (§ 21 Registrierkassensicherungsverordnung).

Derartige Hashwerte werden auch in einer Blockchain angewendet: Um **die Integrität eines Blocks** (d.h. der darin enthaltenen Transaktionen) zu schützen, wird jeder Block mit einem Hash versiegelt. Dieser Hash des aktuellen Blocks kommt sodann (neben dem eigentlichen Inhalt, nämlich diversen Transaktionen) in den Folgeblock. Für diesen Folgeblock wird wieder ein Hash erstellt, welchen den Folgeblock versiegelt (und wiederum in den Block aufgenommen wird).

Durch das repetitive Versiegeln eines Blocks mit einem Hash und die Aufnahme dieses Hashes in den darauffolgenden Block wird erreicht, dass jede Manipulation eines Blocks sich auf alle danach folgenden Blöcke auswirkt. Mit anderen Worten: Wenn ein Block manipuliert wird, ändert sich sein Hash; weil dieser Hash in den Folgeblock kommt, ändert sich auch dessen Hash usw.

Bei Bitcoin kommt das Verfahren SHA-256 zur Anwendung, ebenso wie auch bei der Daten-Zertifizierung.

Hingewiesen werden muss auch noch auf eine Gefahr bei einer Blockchain, nämlich die Gefahr einer 51% Attacke. Bei dieser (auch „double spend attack“ genannt) übernimmt ein Angreifer kurzfristig die Kontrolle über mehr als 50% der Miner und kann in diesem Zeitraum von ihm gehaltene Einheiten der Kryptowährung doppelt ausgeben, oder auch andere Manipulationen vornehmen. Dies muss daher verhindert werden.

Beschreibung System und Funktionsweise

Das System der Daten-Zertifizierung², abrufbar unter mein.wko.at, ermöglicht es durch Anwendung der Blockchain-Technologie zu beweisen, dass elektronische Daten (etwa Personenzertifikate, urheberrechtlich relevante Dokumente, ...) zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert haben und seither nicht verändert wurden. Damit wird die Sicherheit geschaffen, dass zertifizierte Daten nicht manipuliert wurden. Wesentlich ist dabei, dass ausschließlich anonyme Daten (nämlich Prüfsummen bzw. Hashwerte von elektronischen Daten) verarbeitet werden.

Die Funktionsweise ist dabei wie folgt:

Nach Start des Services (siehe Abbildung 1) gibt es entweder die Möglichkeit ein Datenzertifikat zu erstellen oder zu überprüfen, ob die Datei bereits zertifiziert wurde.

Abbildung 1 Service für Datenzertifizierung

Bei Auswahl von „Erstellen“ besteht die Möglichkeit eine Datei auszuwählen (siehe Abbildung 2), von dieser wird ein digitaler Fingerabdruck (Hashwert) in der Blockchain erstellt, in dem der Zeitpunkt der Erstellung festgehalten wird. Nur dieser Fingerabdruck wird an den Server übertragen. Die Inhalte der Dateien werden nicht übertragen. Angemerkt sei, dass prinzipiell alle Dateien verarbeitet werden können, also nicht nur PDF, sondern auch Officedokumente, oder Audio- bzw. Videodateien.

² Der englischsprachige Begriff dafür ist „notarization“, weswegen üblicherweise im Deutschen auch der Begriff Daten-Notarisierung gebräuchlich ist. Aus sozialpartnerschaftlichen Gründen wird bei diesem Service aber der Phantasie-Begriff „Daten-Zertifizierung“ verwendet.



Abbildung 2 Auswahl einer Datei für Zertifizierung

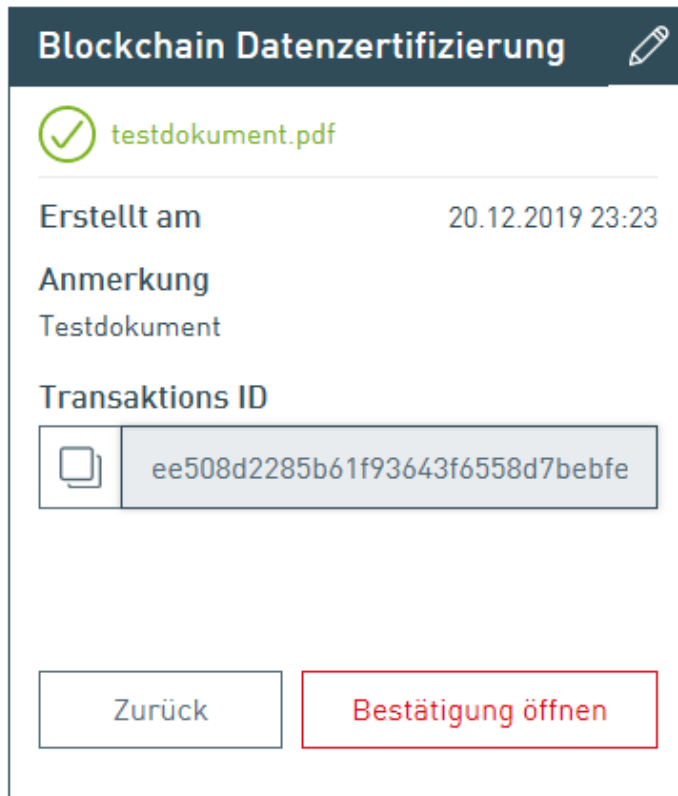


Abbildung 3 Generierung einer Transaktions ID

Das Zertifizierungsservice generiert dabei eine eindeutige Transaktions ID (siehe Abbildung 3), die etwa folgendes Aussehen haben kann:

ee508d2285b61f93643f6558d7bebfe29935c04fba0743f6989d4d395e5fcef0

Außerdem wird ein Bestätigungs-PDF (siehe Abbildung 4) automatisch generiert. Dieses PDF kann lokal abgespeichert werden (wird aber auch automatisch in das persönliche Nachrichtenfach unter mein.wko.at gesendet).



Blockchain Datenzertifizierung - Bestätigung

Erstellt am 20.12.2019 um 23:23:02 Uhr

Zum angegebenen Zeitpunkt wurde der digitale Fingerabdruck (Hashwert) der Datei in der [Blockchain](#) hinterlegt.

Details zur hinterlegten Datei:


Dateiname	testdokument.pdf
Digitaler Fingerabdruck (Hashwert)	9197b77dddcddf915d3c7e22311b91539e5c06d915e38cebde33ec6be794bce6
Anmerkung beim Einbringen	Testdokument
Transaktions-ID zur direkten Verifizierung in der Blockchain	ee508d2285b61f93643f6558d7bebfe29935c04fba0743f6989d4d395e5fcef0


Abbildung 4 Datenzertifizierung-Bestätigung

Für ein zertifiziertes Dokument kann mit der Funktion „Überprüfung“ (siehe Abbildung 5) jederzeit die entsprechende Information abgerufen werden (siehe Abbildung 6), wobei auch ein detaillierter Bericht erzeugt wird (siehe Abbildung 7).

Angemerkt sei, dass falls ein identisches Dokument mehrfach in der Blockchain hinterlegt wurde, auch alle Zeitpunkte angezeigt werden (siehe Abbildung 8).

Blockchain Datenzertifizierung

 Erstellen

 **Überprüfen**



testdokument.pdf 


Abbildung 5 Datenzertifizierung – Überprüfen einer Datei

Blockchain Datenzertifizierung

 testdokument.pdf

Zuletzt erstellt 20.12.2019 23:23
am

Digitaler Fingerabdruck (Hash)

 9197b77dddcddf915d3c7e22311b91

Transaktions-ID


 ee508d2285b61f93643f6558d7bebfe

Abbildung 6 Datenzertifizierung – Angezeigte Informationen bei Überprüfung

- 9 -

Details zum Dokument

testdokument.pdf

Der digitale Fingerabdruck (Hashwert) wurde in der Blockchain gefunden und zuletzt am 20.12.2019 eingebracht.

Der Fingerabdruck lautet:
9197b77dddcddf915d3c7e22311b91539e5c06d915e38cebde33ec6be794bce6

Die Transaktions-ID lautet:
ee508d2285b61f93643f6558d7bebfe29935c04fba0743f6989d4d395e5fcef0

Damit ist bewiesen, dass das Dokument mit diesem Fingerabdruck seit dem Einbringen in das Datenzertifizierungsservice nicht verändert wurde.

Erstellt am
20.12.2019 23:23

Digitaler Fingerabdruck (Hashwert)
9197b77dddcddf915d3c7e22311b91539e5c06d915e38cebde33ec6be794bce6

Transaktions-ID
ee508d2285b61f93643f6558d7bebfe29935c04fba0743f6989d4d395e5fcef0

Abbildung 7 Datenzertifizierung – Überprüfung Details

Details zum Dokument

testdokument.pdf

Der digitale Fingerabdruck (Hashwert) wurde in der Blockchain gefunden und zuletzt am 22.12.2019 eingebracht.

Der Fingerabdruck lautet:
9197b77dddcddf915d3c7e22311b91539e5c06d915e38cebde33ec6be794bce6

Die Transaktions-ID lautet:
d62ce6eb845c7eace8c2091bb29bb19008ce7c2b6fda90fdddc9d4070203e9de

Damit ist bewiesen, dass das Dokument mit diesem Fingerabdruck seit dem Einbringen in das Datenzertifizierungsservice nicht verändert wurde.

Erstellt am
22.12.2019 18:34

Digitaler Fingerabdruck (Hashwert)
9197b77dddcddf915d3c7e22311b91539e5c06d915e38cebde33ec6be794bce6

Transaktions-ID
d62ce6eb845c7eace8c2091bb29bb19008ce7c2b6fda90fdddc9d4070203e9de

Erstellt am
20.12.2019 23:23

Digitaler Fingerabdruck (Hashwert)
9197b77dddcddf915d3c7e22311b91539e5c06d915e38cebde33ec6be794bce6

Transaktions-ID
ee508d2285b61f93643f6558d7bebfe29935c04fba0743f6989d4d395e5fcef0

Abbildung 8 Datenzertifizierung – Überprüfung Details bei mehrfach zertifiziertem Dokument

Wird hingegen ein Dokument überprüft, dass noch nicht in die Blockchain eingetragen wurde, kommt eine entsprechende Meldung, dass das Dokument nicht bestätigt werden konnte (siehe Abbildung 9).

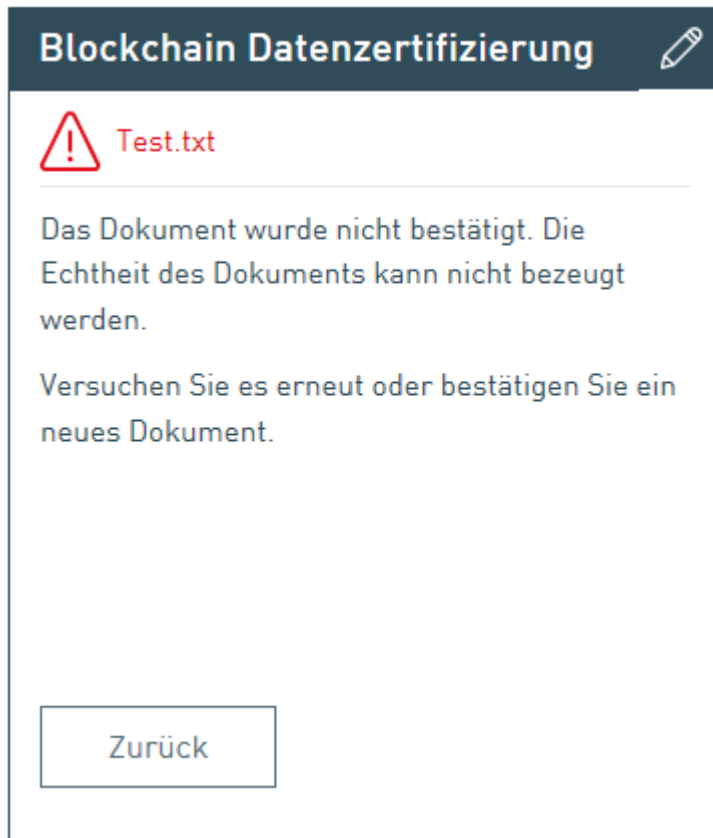


Abbildung 9 nicht bestätigtes Dokument

Verwendete Technologien & Standards

Laut der Beschreibung auf

www.wko.at/service/innovation-technologie-digitalisierung/blockchain.html

wird folgende technische Erklärung abgegeben:

Die verwendete "Blockchain" nennt sich "Austrian Public Service Blockchain" und wird von Institutionen aus dem öffentlichen Bereich gemeinsam betrieben. Derzeit sind es die WKO, das Bundesrechenzentrum und die Stadt Wien. Weitere Teilnehmer z. B. aus dem akademischen Bereich und dem der Datensicherheit kommen demnächst dazu.

Jeder Teilnehmer betreibt einen Blockchain-Knoten, der mit den anderen Knoten synchronisiert wird und trägt damit zur Sicherheit des Gesamtsystems bei. Für die einzelnen Anwendungen sorgt jeder Partner selbst.

Als technische Basis wird "MultiChain" (www.multichain.com) verwendet, eine verbreitete OpenSource Blockchain Plattform. Da die teilnehmenden Knoten alle bekannt sind (man nennt das auch "Konsortium-Chain"), muss kein energieintensives "Proof-Of-Work" Verfahren eingesetzt werden um Konsens bei der Validierung neu hinzukommender Daten-Transaktion bzw. bei der Generierung neuer Blöcke zu erzielen! Daher erfordert der Betrieb unserer einzelnen Blockchaintknoten nicht mehr Strom als jeder andere Webserver.

Darüber hinaus geht aus der Dokumentation hervor, dass als Hash-Verfahren SHA-256 verwendet wird.

In diesem Abschnitt werden daher im Folgenden die Themen MultiChain, Konsortiums-Teilnehmer und Hashverfahren behandelt.

Davor sei aber auch noch angemerkt, dass es auch eine REST-API gibt mit der die Notarisierung erstellt werden kann, nähere Infos dazu können der diesbezüglichen Dokumentation entnommen werden.

MultiChain

MultiChain³ ist eine Open-Source Plattform mit der private Blockchains implementiert werden können. Der komplette Sourcecode ist auf Github verfügbar:

<https://github.com/MultiChain/multichain>

Ein Whitepaper⁴ beschreibt die Implementierung dieser Blockchain, die unter Windows, Linux und Mac lauffähig ist, sie ist prinzipiell ein fix, fertiges Produkt („off-the-shelf platform), dass auch z.B. vom Fraunhofer-Institut als bekannter Vertreter von privaten Blockchains empfohlen wird⁵.

³ www.multichain.com

⁴ Abrufbar unter www.multichain.com/download/MultiChain-White-Paper.pdf

⁵ Z.B. Fraunhofer Whitepaper „Blockchain und Smart Contracts: Effiziente und sichere Wertschöpfungsnetzwerke“, abrufbar unter:

https://www.iml.fraunhofer.de/content/dam/iml/de/documents/101/10_Whitepaper_Blockchain+Smart-Contracts_web.pdf

Als Konsensmechanismus wird „Proof-Of-Authority“ verwendet⁶, dabei handelt es sich in gewisser Weise um eine Weiterentwicklung von „Proof-Of-Stake“, bei dem die Transaktionen von ausgewählten Konsortiums-Teilnehmer abgezeichnet werden müssen. Die Qualität dieses Mechanismus hängt also von der Vertrauenswürdigkeit dieser Teilnehmer ab.

Konsortiums-Teilnehmer

Die Blockchain wird von Institutionen aus dem öffentlichen Bereich gemeinsam betrieben. Derzeit sind es die WKO, das Bundesrechenzentrum und die Stadt Wien.

Das Bundesrechenzentrum ist dabei eine GmbH, die zu 100% im Besitz des Bundes steht und 1997 gegründet wurde. Bei der Gründung wurden die IT-Bereiche des Finanzministeriums ausgegliedert.

Die Konsortiums-Teilnehmer sind daher wohl unzweifelhaft als ausgesprochen vertrauenswürdig einzustufen, insbesondere da sie allesamt auch andere Register verwalten und dies ohne eine technische Garantie wie eine Blockchain.

Hashverfahren

In der Technischen Richtlinie des BSI⁷ TR-02102-1⁸ (Kryptographische Verfahren: Empfehlungen und Schlüssellängen) wird eine Hashfunktion wie folgt definiert:

Eine Funktion $h: M \rightarrow N$, die effizient berechenbar ist und für die M deutlich größer ist als N . h heißt kryptographische Hashfunktion, wenn sie kollisionsresistent und resistent gegen Berechnung erster und zweiter Urbilder ist.

Vereinfacht gesagt, bedeutet dies:

Eine Anwendung einer derartigen Hashfunktion ist dabei eben aus einer Menge von Zeichen (etwa einer Datei) einen eindeutigen Wert zu generieren. Es kann damit der Inhalt einer Datei mit einer einzigen Zeichenkette repräsentiert werden. Jede minimale Veränderung der Zeichenkette führt zu einem anderen Hashwert.

Dabei werden laut BSI folgende Eigenschaften verlangt:

Einweg-Eigenschaft: Für gegebenes $h \in \{0,1\}^n$ ist es praktisch unmöglich, einen Wert $m \in \{0,1\}^*$ mit $H(m) = h$ zu finden.

2nd-Preimage-Eigenschaft: Für gegebenes $m \in \{0,1\}^*$ ist es praktisch unmöglich, einen Wert $m' \in \{0,1\}^* \setminus \{m\}$ mit $H(m) = H(m')$ zu finden.

⁶ Siehe beispielsweise <https://en.bitcoinwiki.org/wiki/Proof-of-Authority> abgerufen am 12.1.2020

⁷ Bundesamt für Sicherheit in der Informationstechnik

⁸ Version 2019-01 vom 22.2.2019, abrufbar unter

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

Kollisionsresistenz: Es ist praktisch unmöglich, zwei Werte $m, m' \in \{0,1\}^*$ so zu finden, dass $m \neq m'$ und $H(m) = H(m')$ gilt.

Basierend auf diese Grundregeln hält das BSI in der TR 02102 fest, dass die folgenden Hashfunktionen als kryptographisch stark gelten:

- SHA-256, SHA-512/256, SHA-384 und SHA-512⁹
- SHA3-256, SHA3-384, SHA 3-512

⁹ siehe Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4) Secure Hash Standard, 2012

Praktische Versuche

Es wurden verschiedenste Dokumente in die Blockchain eingefügt und diese konnten jeweils immer problemlos aufgefunden werden.

Auch wurden die Dokumente mit im Internet verfügbaren SHA-256-Tools¹⁰ verglichen und dabei konnten jeweils die gleichen Hashwerte beobachtet werden.

Testdokument.pdf:

9197b77dddcddf915d3c7e22311b91539e5c06d915e38cebde33ec6be794bce6

Testdokument2.pdf

d9dcd4bbb81c545ecf644e4bb42f9b1acb5027baa831a749078182d7b618fc46

Testdokument3.pdf

9eeb3df75af6bd49959486ec96fa0da6cc92ee9980b306824a7d38c91762a175

Beim Einbringen ist auch eine Transaktions-ID sichtbar, mit der, wie in Abbildung 5 sichtbar, auch die Echtheit überprüft werden kann. Eine Einsicht in den kompletten Blockchain Stream ist allerdings nicht möglich.

¹⁰ https://emn178.github.io/online-tools/sha256_checksum.html und <https://hash.online-convert.com/sha256-generator>

Zusammenfassende Bewertung

In dieser privatgutachterlichen Stellungnahme wurde die „Daten-Zertifizierung“ auf Basis Blockchain, wie sie unter mein.wko.at angeboten wird, untersucht.

Zusammenfassend lässt sich folgendes festhalten:

- Die verwendete Hashmethode SHA-256 gilt laut der BSI-TR 02102 als kryptographisch stark
- Die zugrundeliegende Blockchain-Bibliothek „MultiChain“ ist eine weit verbreitete Open-Source Plattform, die in vielen Quellen empfohlen wird.
- Das Service ist einfach für jedermann handzuhaben.

Es ist daher von einer verlässlichen Möglichkeit, zu beweisen, dass elektronische Daten zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert haben und seither nicht verändert wurden, auszugehen. Nach Ansicht des unterzeichnenden Sachverständigen entspricht dies jedenfalls dem Stand der Technik und kann zum jetzigen Zeitpunkt nicht widerlegt werden.

Dennoch wäre folgender Vorschläge aus Sicht des Sachverständigen sinnvoll:

- Es sollte für jedermann die Möglichkeit geben in den Blockchain Stream Einsicht zu nehmen.

Außerdem ist natürlich festzuhalten, dass der erbrachte Beweis von der Vertrauenswürdigkeit der Konsortiumsteilnehmer abhängt. Im konkreten Falle ist diese wohl aber mit an Sicherheit grenzender Wahrscheinlichkeit gegeben.

Festzuhalten ist, dass es sich bei dieser privatgutachterlichen Stellungnahme um ein Privatgutachten im Auftrag des Vereins AUSTRIAPRO handelt für das, auch im Verhältnis zu Dritten, die allgemeinen Bedingungen des Fachverbandes für Unternehmensberatung und Datenverarbeitung der Bundeswirtschaftskammer, vereinbart sind.

Wir erstatten diesen Bericht aufgrund unserer Prüfung sowie der uns erteilten Auskünfte und vorgelegten Unterlagen nach bestem Wissen.

Haag, Dezember 2019



Dr. Markus Knasmüller

Allgemein beideter und gerichtlich zertifizierter Sachverständiger