Privatgutachterliche Stellungnahme

Dokumenten-Notarisierung
auf Basis Blockchain

erstellt von

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

im Auftrag von

Blockchain Initiative Austria
Anton-Krieger-Gasse 83
A – 1230 Wien

Haag, September 2021

Gegenstand des Gutachtens

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

- Beschreibung System und Funktionsweise (Referenzimplementierung unter https://proof.li)
- Verwendete Technologien & Standards
  - Multichain; Opensource ...
  - Hashwertberechnungen
- Praktische Versuche

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 Dokumenten-Notarisierung des Vereins BCI (Blockchain Initiative Austria)[1]. Mit diesem Service (https://proof.li) lassen sich Dokumente einfach und sicher notarisieren. Unabhängig vom Datenformat erhalten Dateien dabei einen Zeitnachweis, wann sie entstanden sind, vorgelegt oder verändert wurden.

Folgende Themen wurden dabei mit dem Auftraggeber BCI (vertreten durch Dr. Baumann) vereinbart:

- Beschreibung System und Funktionsweise
- Verwendete Technologien & Standards
  - Multichain; Opensource ...
  - Hashwertberechnungen
- Praktische Versuche

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 Verein BCI, wie auch einige Grundlagen zum Thema Blockchain zu präsentieren.

Der Verein "Blockchain Initiative Austria" bezweckt:

- Die Unterstützung des Aufbaus einer sicheren, vertrauenswürdigen und dauerhaften Blockchain-Infrastruktur für die privatwirtschaftliche Nutzung.
- Die Einrichtung einer Plattform zur Organisation und Moderation der Weiterentwicklung von dazu notwendigen Themen (technisch, rechtlich, organisatorisch …).
- Die Unterstützung der Definition und Umsetzung von Anwendungsfällen im Zusammenhang mit Blockchain-Technologien.

Die erste Anwendung, die der Verein aufbaut, ist die sog. "Dokumenten-Notarisierung". Mit Hilfe dieser Anwendung kann die Integrität von elektronischen Dokumenten (d.h. allen Arten von Dateien) sichergestellt werden. Durch die Hinterlegung eines digitalen Fingerabdrucks von Daten in der Blockchain kann später bewiesen werden, dass die Daten zum betreffenden Zeitpunkt in einer bestimmten Form vorgelegen sind und seither nicht verändert wurden. Im öffentlichen Bereich wird dieses Verfahren bereits eingesetzt, nun werden auch sinnvolle privatwirtschaftliche Anwendungen ermöglicht.

Neben einer unter https://proof.li verfügbaren Referenzimplementierung betreiben auch verschiedene Mitglieder ebenfalls eine Anwendung zur Dokumentennotarisierung, derzeit die Firma DEUDAT GmbH (https://node01.deudat.de/) und die Rechtsanwaltspartnerschaft Kosch & Partner Rechtsanwälte GmbH (https://digicert.kosch-partner.at/). Eine vollständige Liste der aktuellen Mitglieder findet sich auf der Webseite des Vereins.

[1] www.bc-init.at

Die für diese Anwendung nötigen Blockchain-Knoten werden von den Vereinsmitgliedern in Form einer sog. „Konsortium-Chain“ betrieben. Dabei entsteht – anders als bei öffentlichen Blockchains – KEIN unnötig hoher Energieverbrauch.

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.
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 Etherum-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.

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 Registrierkassen-sicherheitsverordnung).

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-Notarisierung.

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[2].

[2] Angemerkt sei, dass bei dem in diesem Gutachten untersuchten System durch die Verwendung von Proof Of Authority diese Gefahr nicht gegeben ist, weil eben diese Kontrolle von mehr als 50% verhindert wird.

Beschreibung System und Funktionsweise

Das System der Dokumenten-Notarisierung, abrufbar unter https://proof.li, ermöglicht es durch Anwendung der Blockchain-Technologie zu beweisen, dass elektronische Daten (alle Arten von Dateien) zu einem bestimmten Zeitpunkt in einer bestimmten Form existiert haben und seither nicht verändert wurden. Damit wird die Sicherheit geschaffen, dass notarisierte 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 Service (siehe Abbildung 1) gibt es entweder die Möglichkeit ein Datenzertifikat zu erstellen oder zu überprüfen, ob die Datei bereits zertifiziert wurde.

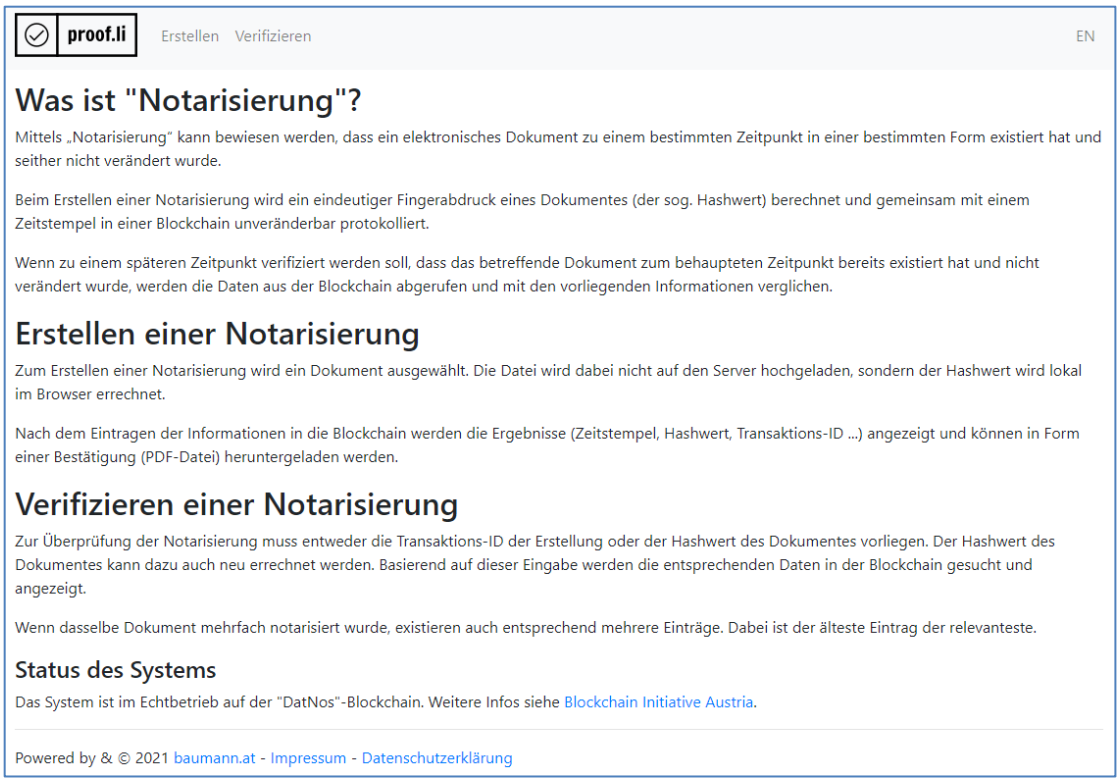


Abbildung 1 Service für Dokumenten-Notarisierung

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, Grafiken, Audio & Video-Dateien, wie auch ZIP-Files etc.

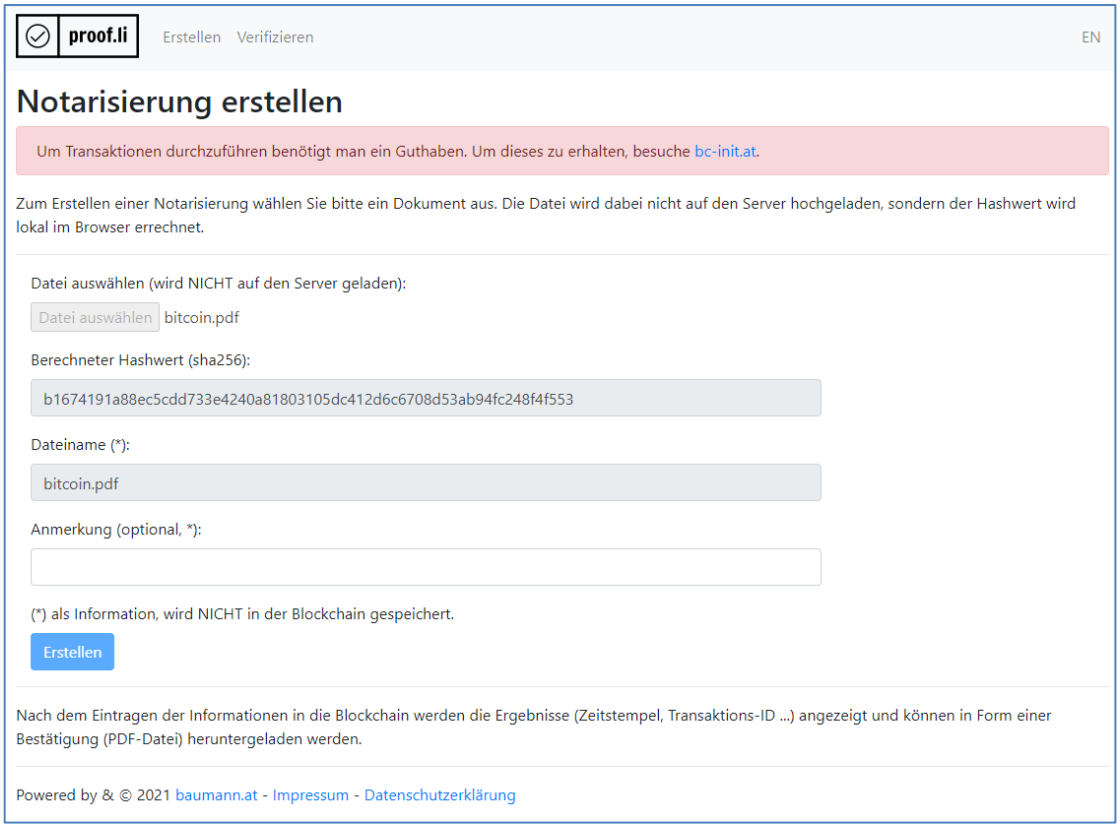


Abbildung 2 Auswahl einer Datei für Notarisierung

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

3ac14f80b09e3cd3da43cb110b6076eba101d4e381f03c26824eeea13875613b

Außerdem wird ein Bestätigungs-PDF (siehe Abbildung 4) automatisch generiert. Dieses PDF kann lokal abgespeichert werden.

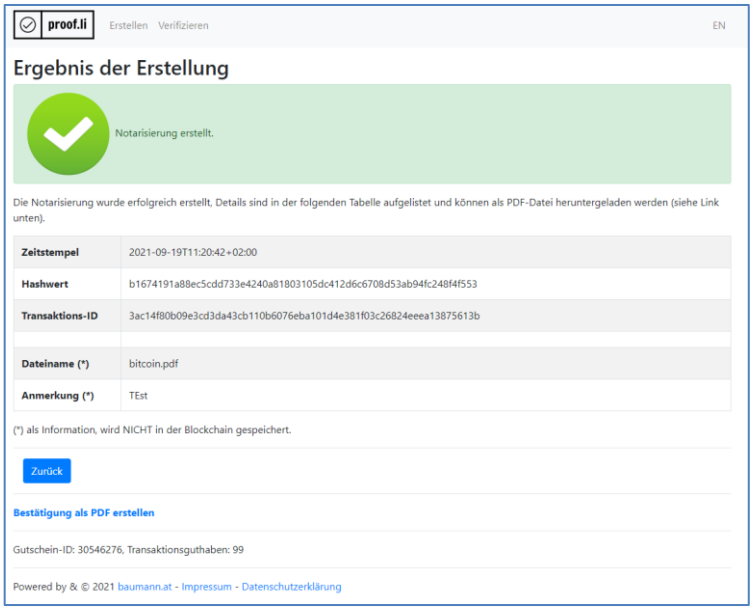
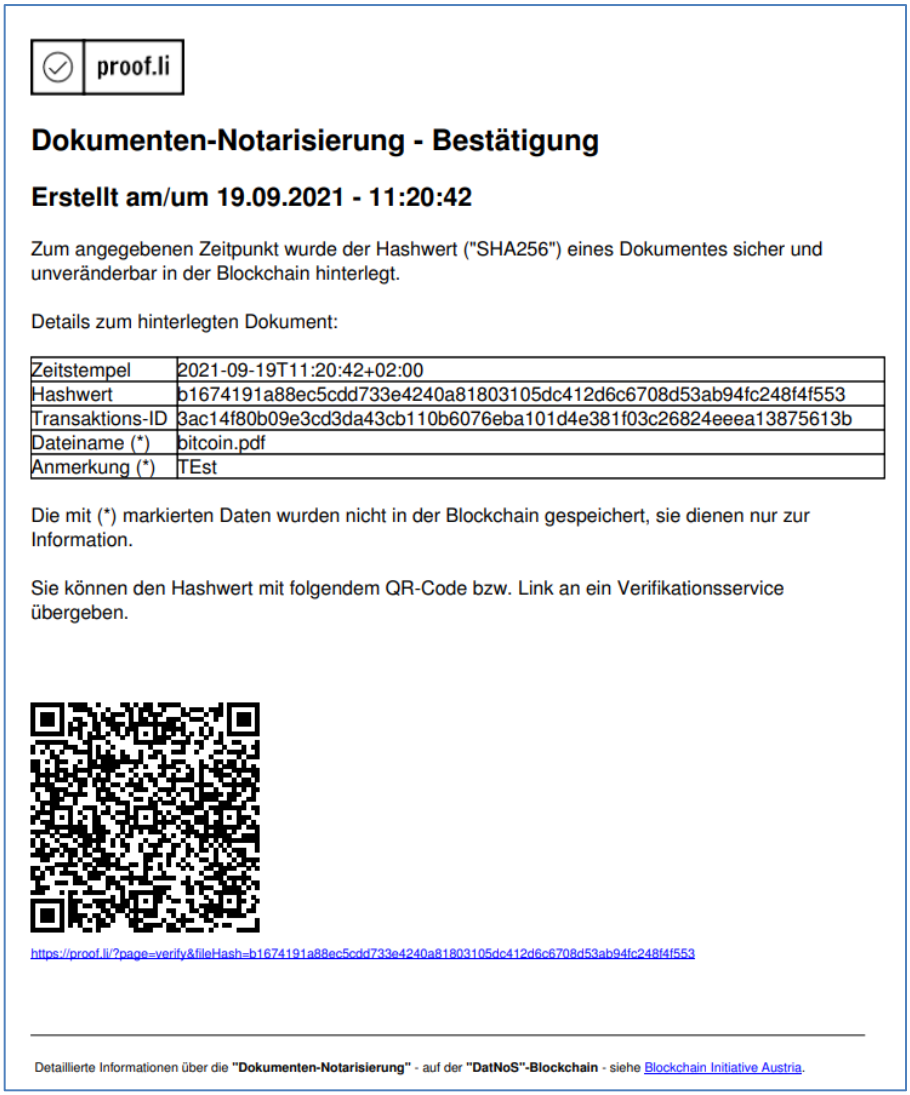


Abbildung 3 Datenzertfizierung-Bestätigung



proof.li

Dokumenten-Notarisierung - Bestätigung

Erstellt am/um 19.09.2021 - 11:20:42

Zum angegebenen Zeitpunkt wurde der Hashwert ("SHA256") eines Dokumentes sicher und unveränderbar in der Blockchain hinterlegt.

Details zum hinterlegten Dokument:

Zeitstempel	2021-09-19T11:20:42+02:00
Hashwert	b1674191a88ec5cdd733e4240a81803105dc412d6c6708d53ab94fc248f4f553
Transaktions-ID	3ac14f80b09e3cd3da43cb110b6076eba101d4e381f03c26824eeea13875613b
Dateiname (*)	bitcoin.pdf
Anmerkung (*)	TEst

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

Sie können den Hashwert mit folgendem QR-Code bzw. Link an ein Verifikationsservice übergeben.

https://proof.li/?page=verify&fileHash=b1674191a88ec5cdd733e4240a81803105dc412d6c6708d53ab94fc248f4f553

Detaillierte Informationen über die **"Dokumenten-Notarisierung"** - auf der **"DatNoS"-Blockchain** - siehe Blockchain Initiative Austria.

Abbildung 4 Bestätigung Dokumenten-Notarisierung als PDF

Für ein notarisiertes Dokument kann mit der Funktion „Verifizieren“ (siehe Abbildung 5) jederzeit die entsprechende Information abgerufen werden (siehe Abbildung 6).

Angemerkt sei, dass falls ein identisches Dokument mehrfach in der Blockchain hinterlegt wurde, auch alle Zeitpunkte angezeigt werden (siehe Abbildung 7).

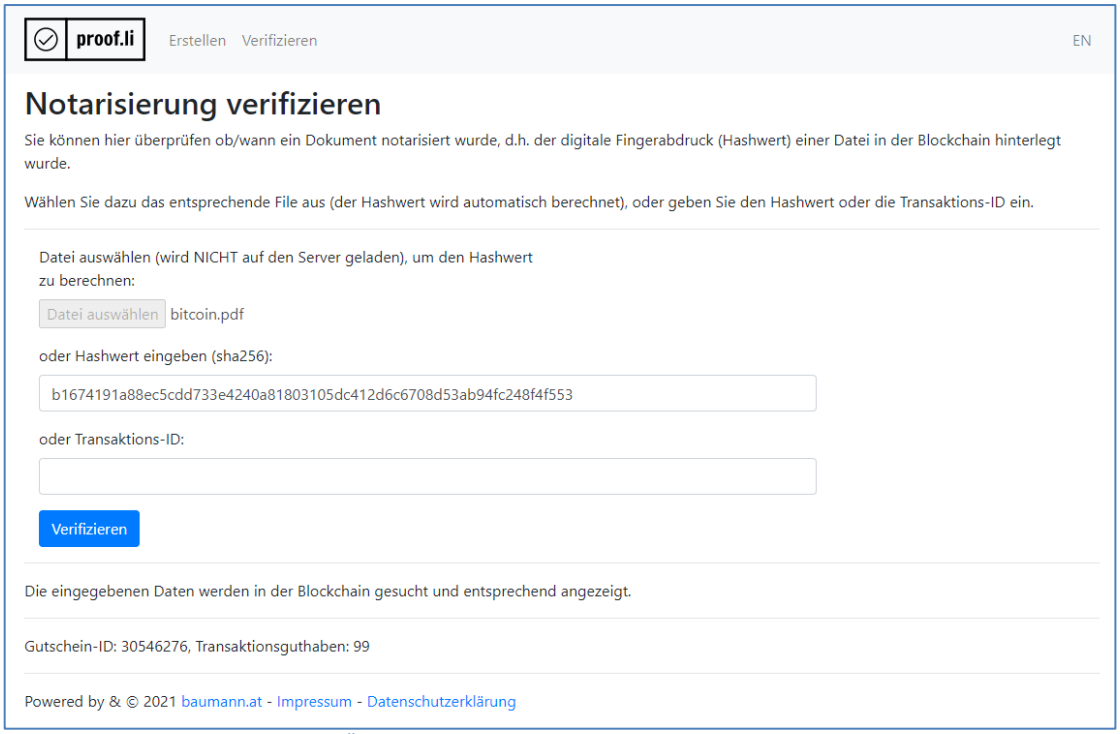


Abbildung 5 Datennotarisierung – Überprüfen einer Datei

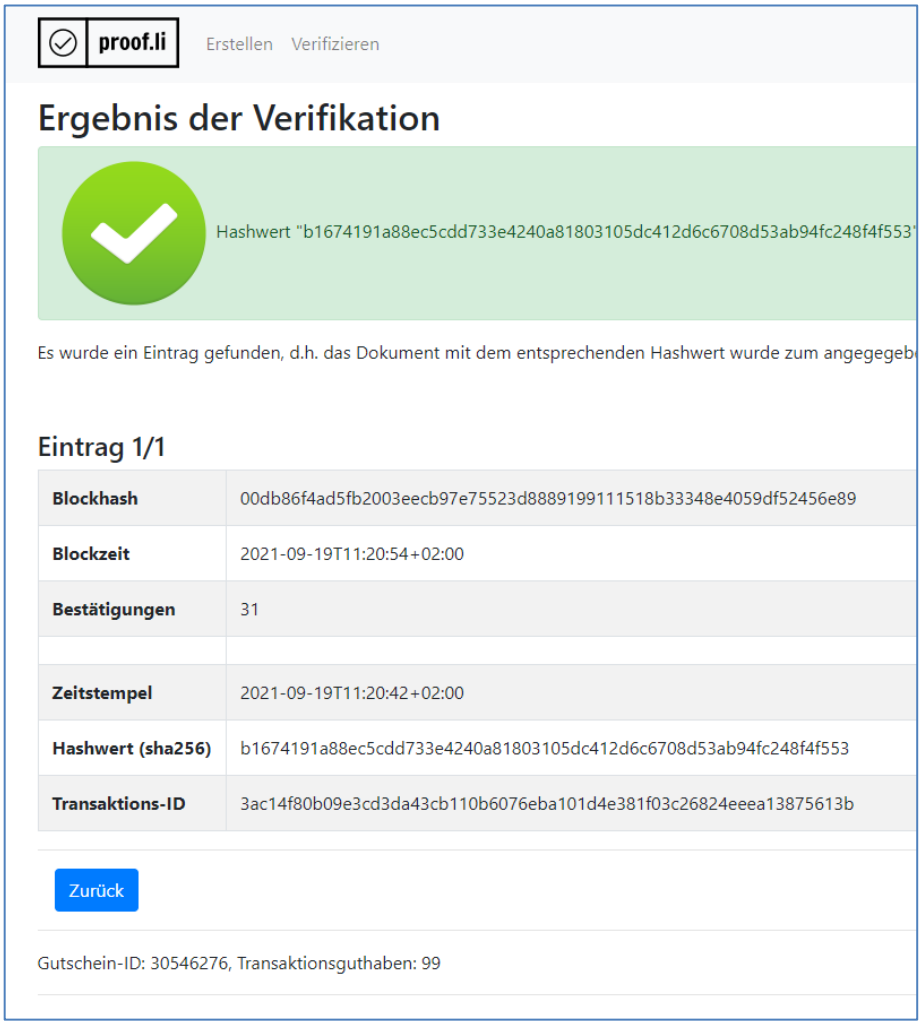


Abbildung 6 Datennotarisierung – Angezeigte Informationen bei Verifikation

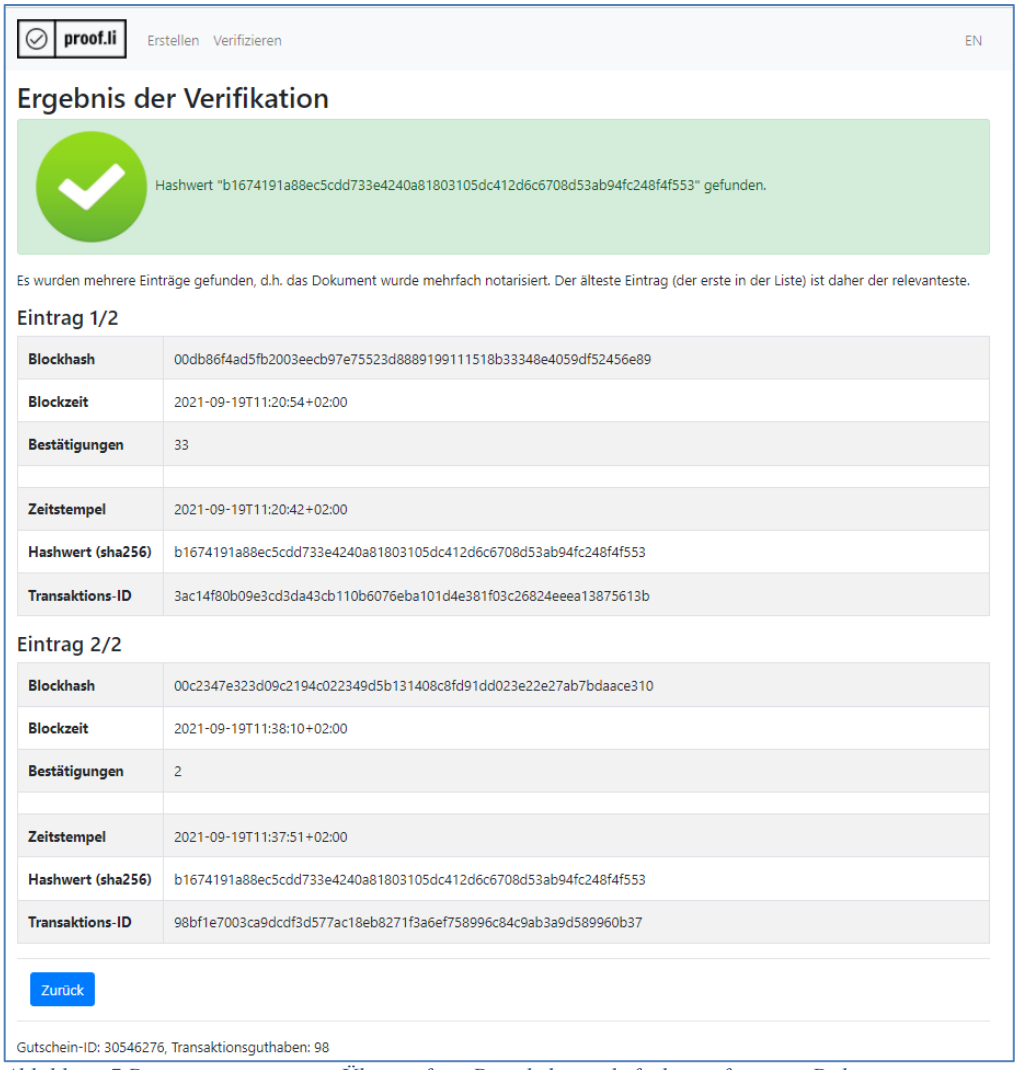


Abbildung 7 Datennotarisierung – Überprüfung Details bei mehrfach zertifiziertem Dokument

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 8).

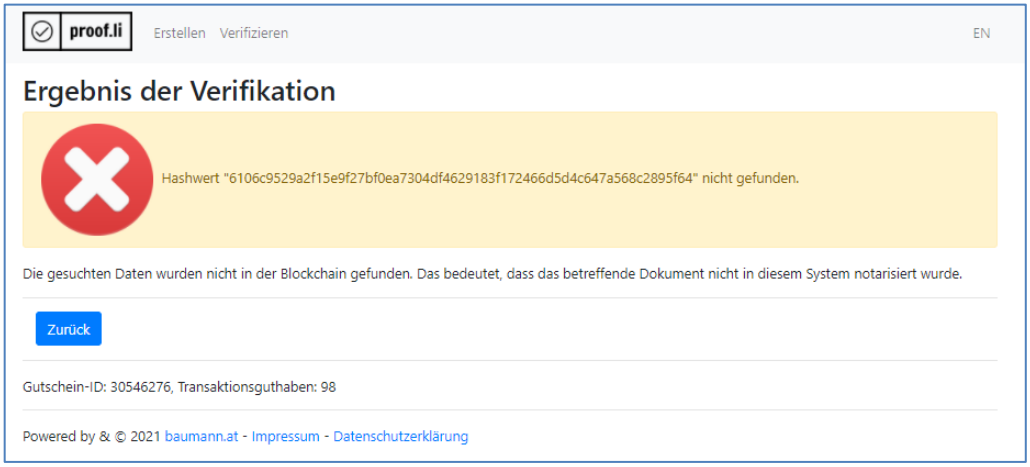


Abbildung 8 nicht bestätigtes Dokument

Verwendete Technologien & Standards

Laut der Beschreibung auf
www.bc-init.at/files/BCI_Beschreibung_20210215.pdf
wird folgende technische Erklärung für die hier zur Anwendung kommende „Konsortium Blockchain“ abgegeben:

„Konsortium Blockchain“: Eine Variante des Aufbaus eines Blockchain-Netzes, wo die Betreiber der Blockchain-Knoten (Nodes) einem „Konsortium“ (hier Verein) angehören. Es wird technisch sichergestellt, dass nur Teilnehmer Daten in die Blockchain schreiben können. Knoten mit Read-Only Zugriff sind möglich (z.B. betrieben durch „unabhängige Dritte“). Ein weiterer Vorteil einer derart aufgebauten Blockchain liegt darin, dass dabei im Gegensatz zu öffentlichen Blockchains kein unnötig hoher Energiebedarf (durch „proof of work“) gegeben ist.

Alt technische Basis für die Blockchain-Umgebung wird das System „MultiChain“ verwendet, wobei die OpenSource Version „Community Edition“ mit der Lizenz GPLv3 eingesetzt wird[3].

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.

MultiChain

MultiChain[4] 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 Whitepaper[5] 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 Frauenhofer-Institut als bekannter Vertreter von privaten Blockchains empfohlen wird[6].

Als Konsensmechanismus wird „Proof-Of-Authority“ verwendet[7], 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.

[3] https://github.com/Multichain/multichain
[4] www.multichain.com
[5] Abrufbar unter www.multichain.com/download/MultiChain-White-Paper.pdf abgerufen am 19.9.2021
[6] 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 abgerufen am 19.9.2021
[7] Siehe beispielsweise www.blockchain-insider.de/was-ist-proof-of-authority-poa-a-943106/ abgerufen am 19.9.2021

Konsortiums-Teilnehmer

Die Blockchain wird von den ordentlichen Mitgliedern des Vereins betrieben, eine jeweils aktuelle Liste ist unter https://bc-init.at/blockchain abrufbar:

Blockchain Nodes

Die Konsortium-Chain "datnos" wird von folgenden Multichain Nodes betrieben (Stand: 14.10.2021)

Node (primäre Adresse)	Mitglied
1Kxq9K5TfEyQXb2rA8aDJdjVxZNcJTxyZzHfSZ	AUSTRIAPRO
1YdUfKkDggxkLE6WMqV36UeJ1Nazbr14cnoiys	baumann.at
1KD9D4fr9w9bmqoFUUtFLkhAv8yDbZ67skzuwj	DEUDAT GmbH
1XJysTLXEntEGCbMCrDoW9Z375HpAWP7QDBhVp	Infinite Trust Digital GmbH
1AapRZuvhK7h4r7cvqyuXVaUTtmvKKWwCsqg9Y	IVM Technical Consultants GmbH
1KmAyPGV99BCi5u9pN1rSJoRyz8G6ZUiWwj7Ec	NIC.at
18WHqcWD5dFPqDoLGf1H5JiUk3vuSZKSbSWRCP	RBK5.com
19s9eNEf7bDTDKGzMDiHvHuD4snyJazjucUp2y	SEC Consult Unternehmensberatung GmbH
1HQNMSpYgTEDNZtkt2vov8CVnLxrkSbn8gXeSh	VIM Internetdienstleistungen GmbH
1RumYCaTEUfHSKoTGB7i9N8WVBc29LrngLZZ3f	WKO (unterstützend)
1VQJMeBDYwT3n24FWjbxeCccmtk5YsTrCqqUqh	Woschitz group GmbH

Der Verein nimmt nur entsprechend geeignete Mitglieder auf. Die Konsortiums-Teilnehmer sind wohl unzweifelhaft als ausgesprochen vertrauenswürdig einzustufen.

Hashverfahren

In der Technischen Richtlinie des BSI[8] TR-02102-1[9] (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:

[8] Bundesamt für Sicherheit in der Informationstechnik
[9] Version 2021-01 vom 24.3.2021, abrufbar unter www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

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´ $\in\{0,1\}^*\backslash\{m\}$ mit H(m)= H(m´) zu finden.

Kollisionsresistenz: Es ist praktisch unmöglich, zwei Werte m, m´ $\in\{0,1\}^*$ so zu finden, dass m $\neq$ m0 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-512[10]
- SHA3-256, SHA3-384, SHA 3-512

Einsicht in die Blockchain

Über https://bc-init.at/docnos/ ist es möglich jederzeit Einsicht in die Blockchain zu nehmen (siehe Abbildung 9). Damit ist eine weitere Sicherheitsstufe umgesetzt.

Publishers	1YdUfKkDggxkLE6WMqV36UeJ1Nazbr14cnoiys
Key 0	id:3b2ac1f6-ae4d-4f18-ab0c-0749444cfe27
Key 1	sha256:b1674191a88ec5cdd733e4240a81803105dc412d6c6708d53ab94fc248f4f553
Key 2	proof.li/c2

JSON data	{
	"timeStamp": "2021-09-19T11:20:42+02:00",
	"client": "proof.li\/c2",
	"version": "DocNoS-v1.1",
	"data": {
	"id": "3b2ac1f6-ae4d-4f18-ab0c-0749444cfe27",
	"hashes": {
	"sha256": "b1674191a88ec5cdd733e4240a81803105dc412d6c6708d53ab94fc248f4f553"
	}
	}
	}

Transaction	3ac14f80b09e3cd3da43cb110b6076eba101d4e381f03c26824eeea13875613b
Blocktime	2021-09-19T11:20:54+02:00
Blockhash	00db86f4ad5fb2003eecb97e75523d8889199111518b33348e4059df52456e89
Confirmations	5430

Abbildung 9 Einsicht in die Blockchain für das in Abbildung 6 notarisierte Dokument

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

Praktische Versuche

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

Auch wurden die Dokumente mit im Internet verfügbaren SHA-256-Tools[11] 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.

[11] 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 „Dokumenten-Notarisierung“ auf Basis Blockchain, wie sie vom Verein „Blockchain Initiative Austria“ 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.

Festzuhalten ist allerdings, dass der erbrachte Beweis von der Vertrauenswürdigkeit der Konsortiumsteilnehmer abhängt. Im konkreten Falle ist diese wohl aber mit an Sicherheit grenzender Wahrscheinlichkeit gegeben. Als zusätzliche Sicherheitsstufe ist auch eine Einsicht in die Blockchain möglich.

Festzuhalten ist, dass es sich bei dieser privatgutachterlichen Stellungnahme um ein Privatgutachten im Auftrag des Vereins „Blockchain Initiative Austria“ 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, Oktober 2021

Dr. Markus Knasmüller
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger

SIGNATURE INFORMATION	**Signatory**	Markus Hermann Knasmüller
	Date/Time-UTC	2021-11-17T16:42:03+01:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signature-verification.gv.at
Note	This document is signed with a qualified electronic signature. According to EU regulation No 910/2014 (eIDAS) it is legally equivalent to a handwritten signature.	