Prioritätsnachweis des Urhebers durch blockchainbasierten Zeitstempel

Heval Mienert/Thomas Hepp/Bela Gipp*

Abstrakt

Der Urheber eines Werks genießt bereits mit der Schöpfung urheberrechtlichen Schutz. Im Gegensatz zum Patent- oder Markenrecht sind keine formellen Voraussetzungen, wie beispielsweise eine Eintragung in das Register beim Deutschen Patent- und Markenamt, für das Entstehen des Urheberrechtsschutzes erforderlich. Sofern Formalien nicht verlangt werden, haben sie auch keine schutzbegründende Funktion. Somit stellt sich die Frage, wie der Urheber eines Werks im Falle eines Rechtsstreits nachweisen kann, dass er das Werk zu einem bestimmten Zeitpunkt bereits geschaffen hatte. Aufgrund der fortschreitenden Digitalisierung ergeben sich für technikaffine Plagiatoren vielfältige Manipulationsmöglichkeiten. So genügen regelmäßig wenige Klicks, um den Autor und den Entstehungszeitpunkt eines digitalen Dokuments zu ändern. Zum sicheren Nachweis der Priorität sollte der digitale Inhalt daher mit einem manipulationssicheren Zeitstempel versehen werden. Anknüpfend an diese Prämisse stellt der Beitrag zunächst den Zeitstempeldienst „OriginStamp" (https://originstamp.org) vor. Beim Zeitstempeldienst „OriginStamp" wird eine Blockchain zur Erstellung und Speicherung von manipulationssicheren Zeitstempeln für digitale Inhalte verwendet, indem der Hash einer Datei in den Transaktionsdatensatz der Kryptowährung integriert wird. Anschließend wird in rechtlicher Hinsicht die Frage erörtert, ob eine Transaktion in einer Blockchain-Datenbank – wie beim Zeitstempeldienst „OriginStamp" – die Voraussetzungen an einen qualifizierten elektronischen Zeitstempel gem. Art. 42 Abs. 1 eIDAS-Verordnung[1] erfüllt. Besondere internationale Aktualität erfährt die Thematik durch die kürzlich veröffentlichten Grundsätze des Supreme People's Court of China zur gerichtlichen Verwertbarkeit digitaler Daten. Der Oberste Volksgerichtshof der Volksrepublik China stellte fest, dass digitale Daten als taugliche Beweismittel vor Gericht bestand haben, wenn sie unter Einsatz der Blockchain-Technologie mit manipulationssicheren Zeitstempeln versehen werden.[2]

I. Zeitstempeldienst „OriginStamp"

Der Zeitstempeldienst „OriginStamp" ermöglicht es Nutzern, ihre digitalen Inhalte mit einem manipulationssicheren Zeitstempel zu versehen.

1. Hashing der Datei

* Der Autor Heval Mienert ist Wissenschaftlicher Mitarbeiter und Doktorrand am Lehrstuhl für Bürgerliches Recht, Handelsrecht, Gewerblichen Rechtsschutz und Urheberrecht von Prof. Dr. Olaf Sosnitza an der Julius-Maximilians-Universität Würzburg. Der Autor Thomas Hepp ist Wissenschaftlicher Mitarbeiter und Doktorrand von Prof. Dr. Bela Gipp an der Universität Wuppertal. Der Autor Bela Gipp (www.gipp.com), Prof. Dr., ist Inhaber des Lehrstuhls für Digitale Medien an der Universität Wuppertal.

[1] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

[2] Vgl. https://www.scmp.com/tech/article/2163487/china-accepts-blockchain-verification-evidence-courtroom.

Zur Erstellung eines beweiskräftigen Prioritätsnachweises ist zunächst der SHA-256-Hash der Datei zu berechnen. Es ist darauf hinzuweisen, dass „OriginStamp“ keinen Zugriff auf die Datei hat, sondern nur den jeweiligen Hash von dem Nutzer zugesendet bekommt. Ein Hash ist das Ergebnis einer Hashfunktion (auch Hashalgorithmus genannt), die aus einer Zeichenfolge beliebiger Länge (z. B. pdf-Dateien) eine Zeichenfolge mit fester Länge errechnet.[3] Plastisch gesprochen fungiert der Hash als digitaler Fingerabdruck einer Datei. Bei „OriginStamp“ findet dabei eine kryptographische Hashfunktion (SHA-256) Verwendung, die es faktisch ausschließt, aus einem Hash auf den Ausgangsinhalt rückzuschließen. Bei der SHA-256 Hash-Funktion handelt es sich um eine mathematische Einwegfunktion, die den Vorteil hat, dass selbst mit hoher Rechenleistung praktisch kein Rückgriff auf den Inhalt der gehashten Datei möglich ist.[4] Ein weiterer Vorteil besteht darin, dass die Länge des Hashes, also des digitalen Fingerabdrucks, nicht mit der Größe der Datei zunimmt, sondern stets auf eine feste Zeichenkette von 64 Zeichen beschränkt ist. Dadurch wird sichergestellt, dass auch sehr große Dateien problemlos mit einem elektronischen Zeitstempel versehen werden können.

2. Einfügen des Hashes in die Blockchain

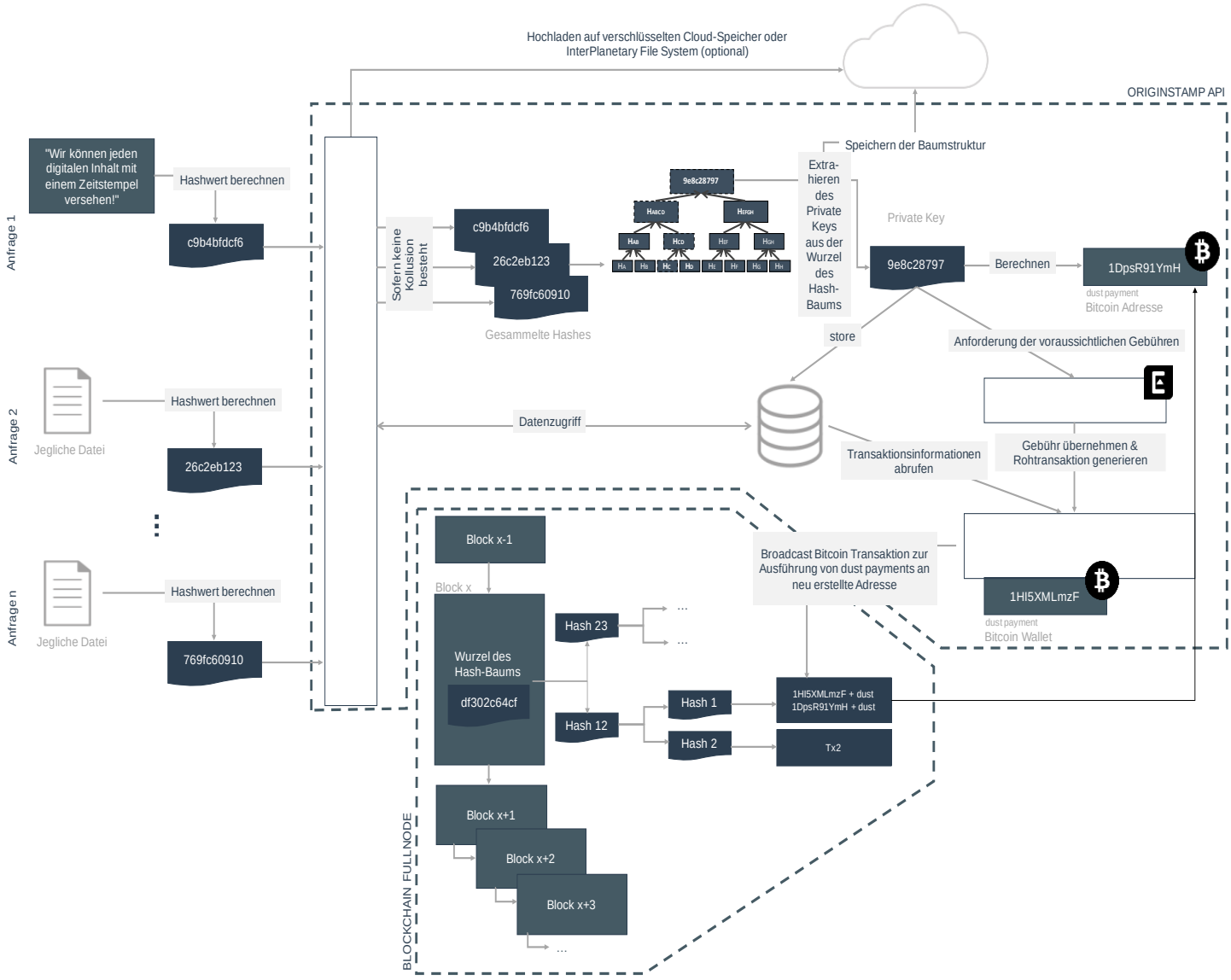
Der berechnete Hash eines digitalen Inhaltes wird daraufhin in den Transaktionsdatensatz der Kryptowährung integriert. Dafür sammelt „OriginStamp“ zunächst die einzelnen Hashes mehrerer Dateien. Aus den einzelnen Hashes erstellt der Zeitstempeldienst einen Top-Hash, der als private Key für die Generierung einer neuen Adresse auf der Blockchain eingesetzt wird. Zur Erstellung des Top-Hashs nutzt „OriginStamp“ die Funktionsweise eines Hash-Baums (auch Merkle tree genannt), bei der es sich um eine kryptographische Baumstruktur handelt, die es ermöglicht, die einzelnen Hashes effizienter zu organisieren. Der Baum ist von unten nach oben aufgebaut und folgt einem definierten Schema. Der Wert eines Knotens wird durch den aggregierten Hash seiner Kinder bestimmt. Die Wurzel des Hash-Baums wird als Top-Hash bezeichnet. Zu der – mithilfe des Top-Hashs berechneten – Adresse wird die kleinste Menge der Kryptowährung gesendet („dust payment“). Der Zeitpunkt der ersten Zahlung, dient als sicherer Nachweis für die Existenz des private Keys zu diesem Zeitpunkt. Jede nachträgliche Änderung der ursprünglichen Dateien hat zur Folge, dass sich auch die jeweiligen eindeutigen Hashes dieser Dateien ändern.

Die Abweichungsempfindlichkeit der eingesetzten Hash-Funktionen ist ein Wesensmerkmal der Blockchain-Technologie, die als dezentrale, verkettete Datenstruktur konzipiert ist. Die Bauteile dieser Datenstruktur sind Blöcke, die Transaktionen enthalten und miteinander durch digitale Fingerabdrücke verkettet sind. Allen Transaktionen ist der genaue Zeitpunkt ihrer Vornahme eingeprägt. Jeder neue Datenblock speichert den Hash des vorangehenden Blocks. Auf diese Weise protokolliert die eingesetzte Blockchain alle jemals gespeicherten Transaktionen in chronologischer Reihenfolge. Sofern ein in dieser Art und Weise verblockter

[3] IETF. *RFC 6234 - US Secure Hash Algorithms b(SHA and SHA-based HMAC and HKDF)*. 2011.

[4] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In: (1989), pp. 33–43. DOI: 10.1145/73007.73011.

und verketteter Datensatz nachträglich verändert wird, entstehen Informationskonflikte mit den nachfolgenden Blöcken, die auf der Basis der ursprünglichen Daten gebildet wurden. Dies ermöglicht die sofortige Identifizierung eines Dateneingriffs. Zu beachten ist dabei zudem, dass die Datenkette dezentral auf den Rechnern der Teilnehmer (Nodes) verteilt gespeichert ist, die ohne zentrale Instanz gleichberechtigt untereinander kommunizieren. Aufgrund der Verbindung aus kryptographischer Verkettung und dezentraler Speicherung erfordert ein unbemerkter Eingriff in die Datenkette enorme Rechenkraft (über 50 % der gesamten Netzwerkrechenleistung), sodass de facto ein lückenloser Manipulationsschutz gewährleistet wird. Abbildung 1 veranschaulicht die Funktionsweise des Zeitstempelvorgangs unter Verwendung des „OriginStamp"-Dienstes:



II. Qualifizierter elektronischer Zeitstempel i.S.d. Art. 42 Abs. 1 eIDAS-Verordnung

Nachdem die technischen Grundlagen des Zeitstempeldienstes „OriginStamp" erläutert wurden, stellt sich nun die rechtliche Frage, ob der – durch die oben beschriebene Vorgehensweise erzeugte – Zeitstempel die Anforderungen an einen qualifizierten elektronischen Zeitstempel gem. Art. 42 Abs. 1 eIDAS-Verordnung erfüllt.

1. Die eIDAS-Verordnung im System des nationalen Rechts

Die eIDAS-Verordnung ist seit dem 18.9.2014 in Kraft. Die materiellen Vorschriften der Verordnung entfalten seit dem 1.7.2016 unmittelbare Rechtswirkungen in allen Mitgliedstaaten. Denn die eIDAS-Verordnung gilt nach Art. 288 Abs. 2 S. 1 AEUV unmittelbar und bedarf keiner Umsetzung in nationales Recht; sie ist somit Teil der deutschen Rechtsordnung. Mit Einführung der eIDAS-Verordnung wurde die Signaturrichtlinie[5], die in Deutschland seit 2001 mit dem Signaturgesetz (SigG)[6] und der Signaturverordnung (SigV)[7] umgesetzt wurde, aufgehoben. Da eine Unionsverordnung keine nationalen Regelungen aufheben kann, galten das SigG und die SigV zunächst weiter. Um diese rechtsunsichere Gemengelage zu beseitigen und das deutsche Recht an die eIDAS-Verordnung anzupassen, trat am 29.7.2017 das Vertrauensdienstegesetz (VDG) als Art. 1 des eIDAS-Durchführungsgesetzes[8] in Kraft. Gleichzeitig traten das SigG und die SigV außer Kraft. Die wesentlichen Regelungen für elektronischen Signaturen, Siegel und Zeitstempel enthält die eIDAS-Verordnung selbst. Dem VDG kommt wegen des Anwendungsvorrangs der Verordnung als unmittelbar geltendes Unionsrecht nur eine präzisierende und ergänzende Funktion zu. Für die rechtliche Einordnung einer Blockchain-Eintragung als elektronischer Zeitstempel sind somit die Vorschriften der eIDAS-Verordnung maßgeblich.

2. Anforderungen an einen qualifizierten elektronischen Zeitstempel gem. Art. 42 Abs. 1 eIDAS-Verordnung

Die eIDAS-Verordnung enthält in Art. 3 eine Reihe von Begriffsbestimmungen. So bezeichnet der Begriff elektronischer Zeitstempel nach Art. 3 Nr. 33 eIDAS-Verordnung „Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren". „OriginStamp" erzeugt einen elektronischen Zeitstempel, indem der Hash einer Datei, die mit einem Zeitstempel versehen werden soll, in eine Blockchain-Transaktion nach der oben beschriebenen Vorgehensweise integriert wird. Da allen Transaktionen der genaue Zeitpunkt ihrer Vornahme eingeprägt ist, gelingt auf diese Weise der Nachweis, dass die gehashte Datei bereits zu diesem Zeitpunkt existiert hat. Somit liegen die Voraussetzungen für einen elektronischen Zeitstempel, wie er in Art. 3 Nr. 33 eIDAS-Verordnung beschrieben ist, vor.

Aus Art. 3 Nr. 34 eIDAS-Verordnung ergibt sich sodann, dass ein qualifizierter elektronischer Zeitstempel ein elektronischer Zeitstempel ist, „der die Anforderungen des Artikels 42 erfüllt". Fraglich ist nun, ob der

[5] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

[6] Gesetz über Rahmenbedingungen für elektronische Signaturen.

[7] Verordnung zur elektronischen Signatur.

[8] Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

von „OriginStamp“ erzeugte Zeitstempel die Anforderungen des Art. 42 Abs. 1 eIDAS-Verordnung erfüllt und somit als qualifizierter elektronischer Zeitstempel klassifiziert werden kann. Art. 42 Abs. 1 eIDAS-Verordnung enthält drei Voraussetzungen, die kumulativ vorliegen müssen. Der elektronische Zeitstempel muss Datum und Zeit so mit den Daten verknüpfen, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist (Art. 42 Abs. 1 lit. a eIDAS-Verordnung). Er muss auf einer korrekten Zeitquelle beruhen, die mit der koordinierten Weltzeit verknüpft ist (Art. 42 Abs. 1 lit. b eIDAS-Verordnung). Schließlich muss der elektronische Zeitstempel mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt werden oder es muss ein gleichwertiges Verfahren verwendet werden (Art. 42 Abs. 1 lit. c eIDAS-Verordnung).

a) Art. 42 Abs. 1 lit. a eIDAS-Verordnung

Art. 42 Abs. 1 lit. a und b eIDAS-Verordnung enthalten die *Integritätsanforderungen*, die an einen qualifizierten elektronischen Zeitstempel gestellt werden. Nach Art. 42 Abs. 1 lit. a eIDAS-Verordnung muss der elektronische Zeitstempel so konzipiert sein, dass die Möglichkeit der unbemerkten Veränderung der mit einem Zeitstempel zu versehenden Datei nach vernünftigem Ermessen ausgeschlossen ist. Zu beachten ist dabei, dass zwar nicht jeder Manipulationsversuch von vornherein ausgeschlossen sein muss, aber dass auf jeden Fall jeder Versuch durch die technische Gestaltung des Verfahrens zwingend auffallen muss.[9]

Der blockchainbasierte Zeitstempeldienst „OriginStamp“ erfüllt diese *Integritätsanforderung* aufgrund der Abweichungsempfindlichkeit der verwendeten Hash-Funktionen und des Mehraugenprinzips der dezentralen Konsensmechanismen. Selbst wenn „OriginStamp“ nicht jede nachträgliche Manipulation der ursprünglichen Datei ausschließen kann, wird aufgrund der Abweichungsempfindlichkeit der eingesetzten Hash-Funktionen sichergestellt, dass eine solche Manipulation zwingend auffällt. Wie bereits oben dargelegt setzt sich der Top Hash, aus dem sich letztlich die Adresse auf der Blockchain ergibt, zu der die kleinste Menge der Kryptowährung gesendet wird, aus den Hashes der zugesandten Dateien zusammen. Sofern die ursprüngliche Datei manipuliert wird, ändert sich auch der eindeutige Hash dieser Datei, der sodann nicht mehr Bestandteil des ursprünglichen Top Hashes ist. Die Veränderung fällt sofort auf, da sich der Zeitstempel mit dem veränderten Top Hash nicht mehr reproduzieren lässt. Zudem ist die Blockchain, in die der Hash einer zugesandten Datei integriert wird, dezentral auf den Rechnern aller Teilnehmer (Nodes) verteilt gespeichert. Aufgrund der dezentralen Speicherung kann der Hash der veränderten Datei de facto auch nicht mehr nachträglich an den Hash der ursprünglichen Datei angepasst und der Eingriff auf diese Weise verschleiert werden.

b) Art. 42 Abs. 1 lit. b eIDAS-Verordnung

[9] *Degen*/*Emmert*, Elektronischer Rechtsverkehr, Rn. 373.

Als weitere *Integritätsanforderung* sieht Art. 42 Abs. 1 lit. b eIDAS-Verordnung vor, dass der elektronische Zeitstempel auf einer korrekten Zeitquelle beruhen muss, die mit der koordinierten Weltzeit verknüpft ist. Dies setzt im Einzelnen voraus, dass die zeitlichen Angaben automatisiert und ohne menschliche Einwirkungsmöglichkeit erfasst werden.[10] Auf diese Weise und der Anknüpfung an die Weltzeit wird sichergestellt, dass der Ersteller des Zeitstempels Datum und Uhrzeit durch eine Änderung der Systemzeit nicht manipulieren kann.[11]

„OriginStamp" bedient sich zur Erstellung eines Zeitstempels der Transaktionen im Rahmen einer Blockchain, da allen Transaktionen der genaue Zeitpunkt ihrer Vornahme eingeprägt ist. Die Blockchain stellt als öffentliche und dezentrale Datenbank die Infrastruktur für diese Transaktionen bereit. Dabei ist der Validierungsvorgang einer Blockchain generell darauf ausgerichtet, ohne die Möglichkeit einer menschlichen Einwirkung abzulaufen. Zudem richtet sich die zeitliche Dokumentation der Transaktionen mangels Anbindung an eine feste Zeitzone auch nach der koordinierten Weltzeit. Daher ist ein „Vordatieren" faktisch unmöglich, sodass die *Integritätsanforderung* des Art. 42 Abs. 1 lit. b eIDAS-Verordnung durch den blockchainbasierten Zeitstempeldienst ebenfalls erfüllt wird.

c) Art. 42 Abs. 1 lit. c eIDAS-Verordnung

In Art. 42 Abs. 1 lit. c eIDAS-Verordnung sind schließlich die *Authentizitätsanforderungen* normiert, die der europäische Gesetzgeber an einen qualifizierten elektronischen Zeitstempel stellt. Demnach muss der Zeitstempel mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt werden oder es muss ein gleichwertiges Verfahren verwendet werden. In technischer Hinsicht sind die – durch die eIDAS-Verordnung als neuen Dienst eingeführten – elektronischen Siegel mit den elektronischen Signaturen vergleichbar. Der rechtliche Unterschied ist die Zuordnung zu einer juristischen anstatt einer natürlichen Person.[12] Während eine natürliche Person mit einer elektronischen Signatur eine Willenserklärung abgeben kann, dient das elektronische Siegel einer juristischen Person als Herkunftsnachweis. Alternativ kann auch ein „gleichwertiges Verfahren" verwendet werden. Eine inhaltliche Präzisierung dieser Generalklausel erfolgt durch den Erwägungsgrund Nr. 62 der eIDAS-Verordnung. Der europäische Gesetzgeber geht darin davon aus, dass in Zukunft auch neue Technologien entwickelt werden, die für Zeitstempel ein gleichwertiges Sicherheitsniveau gewährleisten können wie fortgeschrittene elektronische Signaturen oder Siegel. Somit spielt es im Ergebnis keine Rolle, ob der – durch die oben beschriebene Vorgehensweise erzeugte – Zeitstempel durch die Verwendung einer fortgeschrittenen elektronischen Signatur, eines fortgeschrittenen elektronischen Siegels oder eines gleichwertigen Verfahrens Authentizität erlangt, da sich die einzelnen Anforderungen inhaltlich weitestgehend decken („gleichwertiges Sicherheitsniveau"). Die zentrale

[10] *Jandt*, NJW 2015, 1205, 1207.

[11] *Jandt*, NJW 2015, 1205, 1207.

[12] *Jandt*, NJW 2015, 1205, 1206.

Voraussetzung besteht letztlich in der Identifizierung der beteiligten (natürlichen oder juristischen) Personen.[13] Aus der Lektüre des Art. 26 lit. b und Art. 36 lit. b eIDAS-Verordnung ergibt sich, dass der Unterzeichner beziehungsweise Siegelersteller aus den Informationen der Signatur beziehungsweise des Siegels selbst bestimmbar sein muss. Die Ermöglichung einer solchen Identifizierung hängt im Wesentlichen von der im Einzelfall eingesetzten Blockchain-Konfiguration ab. Die bloße Repräsentation der Netzwerkteilnehmer durch die Hashwerte ihrer öffentlichen Schlüssel dürfte für eine Identifizierung nach den oben genannten Vorschriften generell nicht ausreichend sein. Sofern die eingesetzte Blockchain-Konfiguration jedoch vorsieht, dass sich die Beteiligten mit ihrem Klarnamen registrieren müssen, ist die Authentizität des blockchainbasierten Zeitstempels zu bejahen.

Die Konfiguration des Zeitstempeldienstes „OriginStamp" möchte eine solche Registrierung mit Klarnamen aus datenschutzrechtlichen Gründen gerade vermeiden. Zudem lässt sich nicht mit Sicherheit überprüfen, ob sich der Nutzer auch mit seinem korrekten Klarnamen registriert. Im Hinblick auf die Manipulationssicherheit soll „OriginStamp" auch nur Zugriff auf die jeweiligen Hashs und nicht auf die Dateien als solche haben. Um eine nachträgliche – den datenschutzrechtlichen Bestimmungen genügende – Identifizierung sicherzustellen, können die Urheberinformationen bereits selbst im Dokument hinterlegt werden. Auf diese Weise werden diese Informationen selbst Teil des Hashs und somit auch des Zeitstempels. Dies reicht jedoch nicht aus, um die *Authentizitätsanforderungen* des Art. 42 Abs. 1 lit. c eIDAS-Verordnung zu erfüllen.

III. Fazit

Der blockchainbasierte Zeitstempeldienst „OriginStamp" ermöglicht es Nutzern, ihre digitalen Inhalte mit einem manipulationssicheren Zeitstempel zu versehen. Der Urheber eines Werks ist daher nicht mehr – wie im 19. Jahrhundert noch üblich – darauf angewiesen, Briefe an sich selbst zu versenden, um die dabei abgestempelten Briefmarken als Zeitstempel nutzen zu können. Aufgrund der manipulationssicheren, dezentralen Datenstruktur der verwendeten Blockchain-Technologie werden die vom europäischen Gesetzgeber in Art. 42 Abs. 1 eIDAS-Verordnung normierten Vorgaben hinsichtlich der Integrität eines qualifizierten elektronischen Zeitstempels eingehalten.

Die Konfiguration des Zeitstempeldienstes „OriginStamp" erfüllt jedoch nicht die *Authentizitätsanforderungen* des Art. 42 Abs. 1 lit. c eIDAS-Verordnung. Dies wird aus Gründen der Manipulationssicherheit und des Datenschutzes bewusst in Kauf genommen. Wie bereits oben dargelegt existieren andere Möglichkeiten, um eine nachträgliche Identifizierung vorzunehmen. Zwar geht der europäische Gesetzgeber mit seiner Generalklausel („gleichwertiges Verfahren") davon aus, dass in Zukunft auch neue Technologien entwickelt werden, die für Zeitstempel ein gleichwertiges Sicherheitsniveau gewährleisten können wie fortgeschrittene elektronische Signaturen oder Siegel. Sofern die Identifizierung der Nutzer aber wie bei elektronischen Signaturen oder Siegeln erfolgen muss, werden es blockchainbasierte

[13] Vgl. Art. 26 lit. b eIDAS-Verordnung für fortgeschrittene elektronische Signaturen und Art. 36 lit. b eIDAS-Verordnung für fortgeschrittene elektronische Siegel.

Zeitstempel unter Zugrundelegung einer strengen Gesetzesauslegung in Zukunft schwer haben, die *Authentizitätsanforderungen* des Art. 42 Abs. 1 lit. c eIDAS-Verordnung zu erfüllen. Daher wäre hier – aufgrund des enormen Zeitstempelpotenzials der Blockchain-Technologie – eine rechtliche Nachjustierung durch den europäischen Gesetzgeber sinnvoll.