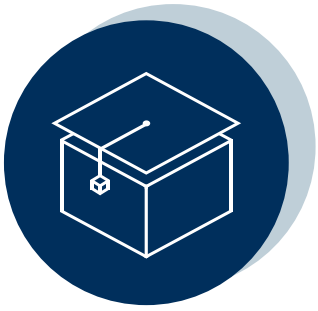


BISE Student

https://bise-student.io

BACHELOR'S THESIS

Proof of Existence als Teil eines Blockchain-basierten Open-Science-Ökosystems

Eine Momentaufnahme und Evaluation technisch-infrastruktureller Aspekte

Publication Date: 2022-09-06

Author
Nicolas BACH
Hochschule der Medien
Stuttgart, Germany
nicolas.bach@posteo.de
0xE02Ace754BE8D37A5107E1f8bA145c2d904AbA60

Abstract

Proof of Existence (PoE) wird seit über zehn Jahren als Blockchain-basiertes Verfahren eingesetzt, um unabhängig von vertrauenswürdigen Dritten und ohne die Offenlegung von Inhalten manipulationssicher nachzuweisen, dass Dokumente oder andere Daten zu einem bestimmten Zeitpunkt existieren. Auch die Open-Science-Community setzt inzwischen in bestimmten Anwendungsfällen auf die Blockchain-Technologie, da diese zur Stärkung von Transparenz, Integrität und Reproduzierbarkeit in Wissenschaft und Forschung beitragen kann. Diese Arbeit geht der Frage nach, ob sich PoE-Verfahren für den Einsatz in einer auf Open Science ausgerichteten Infrastruktur eignen. Zuerst werden technisch-infrastrukturelle Eigenschaften von PoE anhand Erläuterung zugrundeliegender kryptografischen Verfahren, Trusted Timestamping und relevanter Aspekte der Blockchain-Technologie hergeleitet. Weiter werden Grundlagen eines Blockchain-basierten Open-Science-Ökosystems dargelegt und daraus entsprechende Kriterien zur Auswahl eines auf Open Science ausgerichteten...

Keywords: Blockchain, Open Science, Forschungsdaten

Submission Date: 2022-08-22
Submission Contract: 0xc851F9d56d1f9804fa3B9769384da41973fab2b9

Proof of Existence als Teil eines Blockchain-basierten Open-Science-Ökosystems

Eine Momentaufnahme und Evaluation technisch-infrastruktureller Aspekte

Bachelorarbeit

im Studiengang
Bibliotheks- und Informationsmanagement
/ Informationswissenschaften

vorgelegt von

Nicolas Bach
Matr.-Nr.: 36974

am 4. Juli 2022
an der Hochschule der Medien Stuttgart

Erstprüfer:	Prof. Magnus Pfeffer
Zweitprüfer:	Prof. Markus Hennies
Praxisbetreuer:	Dirk Eisengräber-Pabst

Ehrenwörtliche Erklärung

„Hiermit versichere ich, Nicolas Bach, ehrenwörtlich, dass ich die vorliegende Bachelorarbeit (bzw. Masterarbeit) mit dem Titel: „Proof of Existence als Teil eines Blockchain-basierten Open-Science-Ökosystems: Eine Momentaufnahme und Evaluation technisch-infrastruktureller Aspekte“ selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht. Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden.

Ich habe die Bedeutung der ehrenwörtlichen Versicherung und die prüfungsrechtlichen Folgen (§ 26 Abs. 2 Bachelor-SPO (6 Semester), § 24 Abs. 2 Bachelor-SPO (7 Semester), § 23 Abs. 2 Master-SPO (3 Semester) bzw. § 19 Abs. 2 Master-SPO (4 Semester und berufsbegleitend) der HdM) einer unrichtigen oder unvollständigen ehrenwörtlichen Versicherung zur Kenntnis genommen.“

Stuttgart, 04.07.2022

Kurzfassung

Proof of Existence (PoE) wird seit über zehn Jahren als Blockchain-basiertes Verfahren eingesetzt, um unabhängig von vertrauenswürdigen Dritten und ohne die Offenlegung von Inhalten manipulationssicher nachzuweisen, dass Dokumente oder andere Daten zu einem bestimmten Zeitpunkt existieren. Auch die Open-Science-Community setzt inzwischen in bestimmten Anwendungsfällen auf die Blockchain-Technologie, da diese zur Stärkung von Transparenz, Integrität und Reproduzierbarkeit in Wissenschaft und Forschung beitragen kann. Diese Arbeit geht der Frage nach, ob sich PoE-Verfahren für den Einsatz in einer auf Open Science ausgerichteten Infrastruktur eignen. Zuerst werden technisch-infrastrukturelle Eigenschaften von PoE anhand Erläuterung zugrundeliegender kryptografischen Verfahren, Trusted Timestamping und relevanter Aspekte der Blockchain-Technologie hergeleitet. Weiter werden Grundlagen eines Blockchain-basierten Open-Science-Ökosystems dargelegt und daraus entsprechende Kriterien zur Auswahl eines auf Open Science ausgerichteten PoE-Verfahrens formuliert und darauf hin zwei repräsentative PoE-Dienste evaluiert. In der Evaluation wird der Bitcoin-basierte PoE-Dienst OpenTimestamps dem Zertifizierungsdienst für Forschungsdaten der Ethereum-basierten Wissenschafts-Blockchain Bloxberg gegenübergestellt, dabei ihre technischen Eigenschaften sowie die Anschlussfähigkeit an ein Blockchain-basiertes Open-Science-Ökosystem untersucht. Im Ergebnis liegen beide PoE-Dienste gleichauf. Allerdings zeigen sich deutliche Unterschiede im Verhältnis zum Vertrauen, dem Grad der Dezentralisierung und dem Ressourcenverbrauch. Abschließend diskutiert die Arbeit ausgemachte Defizite der Attestierung bei PoE-Diensten sowie mögliche Sicherheitsbedenken. Zudem wird ein Ausblick auf weitere Forschungsansätze gegeben.

Schlagwörter: Blockchain, Open Science, Forschungsdaten, Proof of Existence, OpenTimestamps, Bloxberg, Evaluation

Abstract

For more than ten years, Proof of Existence (PoE) is used as a blockchain-based method to provide tamper-resistant evidence that documents or other data exist at a certain point of time, independently of trusted third parties and without revealing any content to such. Nowadays, there is also recognition within the open science community that there are use cases for leveraging blockchain technology to foster transparency, integrity, and reproducibility in science and research. In this work, the question is addressed of whether PoE techniques are suitable for use in an open science infrastructure. First, the technical infrastructural characteristics of PoE are derived by explaining the underlying cryptographic methods, trusted timestamping, and relevant aspects of blockchain technology. Further, the fundamentals of an blockchain-based open science ecosystem are outlined. From this, a set of criteria for selecting an open science-focused PoE method are formulated, in order to evaluate two representative PoE services. For evaluation, Bitcoin-based PoE service OpenTimestamps and the research object certification service of the Ethereum-based scientific blockchain project Bloxberg are compared by examining their technical characteristics and applicability towards an blockchain-based open science ecosystem. In conclusion, both PoE services are equally suited, but it can be shown that there are fundamental differences in terms of the relationship to trust, the degree of decentralization, and resource consumption. Finally, the work discusses identified drawbacks in relation to the attestation with PoE services as well as possible security concerns, and an outlook on further research approaches is given.

Keywords: Blockchain, Open Science, Research Data, Proof of Existence, OpenTimestamps, Bloxberg, Evaluation

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface
BIP	Bitcoin Improvement Proposal
BLIP	Bloxberg Improvement Proposals
dApp	Decentralized Application
DLT	Distributed Ledger Technology
DPKI	Decentralized Public Key Infrastructure
DSGVO	Datenschutz-Grundverordnung
IPFS	InterPlanetary File System
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
PoA	Proof of Authority
PoE	Proof of Existence
PoS	Proof of Stake
PoW	Proof of Work
REST	Representational State Transfer
RFC	Request for Comments
RPC	Remote Procedure Call
TTP	Trusted Third Party
TSS	Timestamping Service

1 Einführung

Überlegungen zum Einsatz der Blockchain-Technologie haben in den letzten Jahren den Einzug in viele Bereiche der Wirtschaft und Gesellschaft gehalten, vom Finanzsektor über die Industrie (Prinz et al., 2018, S. 311), Öffentliche Verwaltungsbehörden (Guckelberger, 2019, S. 134–135) bis hin zu Bibliotheken (Oyelude, 2019, S. 17–18) und auch in die Wissenschaft (Kosmarski, 2020, S. 10).

Auch seitens Informationswissenschaftler*innen wird das Thema seither diskutiert, etwa wies Lambert Heller (2019) auf dem 7. Bibliothekskongress in Leipzig bei seiner Vorstellung der „Blockchain als öffentliche Logfile der Wissenschaft“ auf die „Entzerrung der Anreizstruktur durch Disintermediation“ hin: „die tatsächlich Beteiligten informieren öffentlich direkt über ihren jeweiligen Beitrag“ (S. 16).

2017 wurde durch den Blockchain-Forscher Sönke Bartling die Blockchain-for-Science-Initiative[1] gegründet und im November 2018 die „1st International Conference on Blockchain for Science, Research and Knowledge Creation“ in Berlin veranstaltet. Bartling sieht in der Blockchain-Technologie das Potenzial, das wissenschaftliche Publikationswesen, die Forschungsförderung und Forschungsfinanzierung zu revolutionieren und sprach sich für die Zusammenarbeit aller Blockchain-Projekte für die Wissenschaft aus, um so ein „wirklich offenes ‚blockchainified Science Ecosystem‘“ zu schaffen. (Kemp, 2018, S. 332, 337.)

In ihrer umfassenden Überblickstudie zur potenziellen Anwendung der Blockchain-Technologie im Bereich Open Science haben Leible et al. (2019, S. 13) dann nachgewiesen, dass sich diese in ihrem aktuellen technischen Stadium bereits vorteilhaft hinsichtlich der Reproduzierbarkeit von Forschungsergebnissen, der Transparenz von Forschungsprozessen und auch zur Nachverfolgung von Forschungsobjekten einsetzen ließe.

Die Blockchain-Technologie hat sich seit der Erfindung durch Satoshi Nakamoto vor mehr als einem Jahrzehnt (Nakamoto, 2008) als eine transparente und bewährte Methode zur manipulationssicheren Verifizierung und dezentralen Speicherung von Daten etabliert (Tasca & Tessone, 2019, S. 1–2). Die fünf Jahre später durch das Ethereum-Projekt implementierten Smart Contracts (Buterin, 2014) ermöglichen die automatisierte Ausführung von individuellen Vorgängen auf einer Blockchain. Sobald diese auf die Blockchain geschrieben wurden, sind sie ebenfalls manipulationssicher und permanent auf dieser vorhanden und werden nur noch über die Blockchain selbst ausgeführt. (Tasca & Tessone, 2019, S. 6.)

Ethereum diente dann Anfang 2019 auch als Code-Basis für Bloxberg[2], die erste internationale Blockchain für die Wissenschaft. Sie wird von einem Konsortium aus etablier-

1 https://www.blockchainforscience.com

2 https://bloxberg.org

ten Wissenschaftsorganisationen und Forschungseinrichtungen föderal betrieben und stellt der Wissenschafts-Community eine Plattform für dezentrale Applikationen (dApps) zur Verfügung (Kleinfercher et al., 2020, S. 4). Hier wird auch auf die Funktion der Smart Contracts zurückgegriffen (Kleinfercher et al., 2020, S. 13).

Ein zentraler Aspekt im wissenschaftlichen Publikationswesen ist die Sicherstellung eines Nachweises über Existenz, Autorenschaft und Herkunft von Forschungsoutput. Vor der Erfindung des Trusted Timestampings (Haber & Stornetta, 1991) verschriftlichten Wissenschaftler*innen ihre Ideen und schickten diese sich selbst per Post zu oder es wurden Schriftstücke bei einem Notar hinterlegt. Über einen Eintrag auf einer Blockchain lässt sich nun heutzutage kryptografisch nachweisbar sichern, dass digitale Dokumente oder andere beliebige Daten zu dem Zeitpunkt in der jeweiligen Dateifassung existiert haben, auch Proof of Existence (PoE) genannt. (Härer & Fill, 2020, S. 2–3.)

PoE war nach dem Bereich der Transaktion von Werten durch Kryptowährungen bzw. Crypto-Coins einer der ersten Anwendungsfälle der Blockchain-Technologie, wie es sich etwa in der Geschichte von OriginStamp nachzeichnen lässt (Gipp et al., 2015, S. 2–4). Auch bei Bloxberg wurde als eine der ersten dApps eine Implementierung zur Zertifizierung von Forschungsdaten bereitgestellt (Kleinfercher et al., 2020, S. 21–22).

Aktuell wird an Konzepten zur Integration von PoE in den gesamten Forschungsworkflow gearbeitet, die auch die Anbindung an dezentrale Speicherlösungen wie IPFS (InterPlanetary File System) in Betracht ziehen (Wittek et al., 2021).

2 Zielsetzung der Arbeit und Vorgehensweise

An dem Punkt des aktuellen Forschungsstands (siehe vorheriger Abschnitt) setzt die vorliegende Arbeit an. Sie will anhand gewisser Kriterien repräsentative PoE-Methoden untersuchen, inwiefern diese den Anspruch erfüllen, in einer Open-Science-Infrastruktur betrieben werden zu können. Entsprechend lautet die Forschungsfrage: Können die auf Blockchain basierten Proof-of-Existence-Lösungen den Kriterien einer auf Open Science ausgerichteten technischen Infrastruktur entsprechen?

Das methodische Vorgehen, mit der der Forschungsfrage nachgegangen werden soll, setzt auf eine Evaluation ausgewählter PoE-Verfahren, die anhand eines der wissenschaftlichen Fachliteratur entnommenen und auf die Anforderungen von PoE angepassten Kriterienkatalogs eingeordnet und verglichen werden.

Der zugrundeliegende Forschungsstand zur Verknüpfung von Blockchain und Open Science sowie der technischen Hintergründe zur Blockchain-Technologie, Trusted Timestamping und Proof of Existence werden hauptsächlich über Sekundärquellen, also wissenschaftliche Literatur in Form von Aufsätzen und Büchern erhoben. Die Einholung der Informationen über die ausgewählten PoE-Verfahren wird überwiegend auf Primärquellen, also Dokumentationen, Webseiten und sonstigen Veröffentlichungen der Entwickler*innen basieren.

Individuelle Ansichten oder empirische Erhebungen sind bei dem Thema Proof of Existence aktuell unerheblich, weil es dafür bisher noch zu wenig Adoption durch wissenschaftliche Einrichtungen erfahren hat. Es kann auch davon ausgegangen werden, dass es dem Anwender*innenkreis (Forschenden oder anderen Stakeholdern) gleichgültig ist, ob bei der Verifizierung ihres Forschungsoutputs eine Blockchain eingesetzt wird oder eine andere Technologie, weil es ihnen allein um eine möglichst effiziente und komfortable Lösung geht. Aus diesem Grund richtet sich die Evaluation, die in dieser Arbeit vorgenommen wird, auch hauptsächlich an die Verantwortlichen, die im Bereich der Forschungsinfrastruktur (z. B. in Forschungsinstituten, angeschlossenen Informationseinrichtungen oder allgemein wissenschaftlichen Bibliotheken) arbeiten und dort die Entscheidung darüber treffen müssen, welche Mittel sie einsetzen, um solch einen Dienst zu erbringen.

Im Schlussteil werden aus einem Vergleich der evaluierten Praxisbeispiele Handlungsempfehlungen abgeleitet und ein Fazit gezogen.

Bei der Bearbeitung des Themas trifft die Arbeit im Vorfeld folgende Einschränkungen:

- Der Fokus liegt primär auf der Blockchain-Technologie und nicht auf DLT (Distributed Ledger Technology) im Allgemeinen, da Methoden, die nicht auf dem Blockchain-Prinzip beruhen, nicht unbedingt die Eigenschaft der Unveränderbarkeit als zentrale Grundvoraussetzung für Trusted Timestamping mitbringen. Sonstige Blockchain-ähnliche Systeme (wie z. B. verteilte Dateisysteme) werden nur behan-

delt, insofern sie einen signifikanten Bestandteil an dem PoE-Prozess einnehmen können.

- Des Weiteren werden bei der Evaluation von repräsentativen Beispielen ausschließlich nicht-kommerzielle Open-Source-Lösungen herangezogen. Anbieter proprietärer Lösungen erzeugen eine Abhängigkeit, die nicht im Sinne des Gedankens von Dezentralisierung stehen kann. Kund*innen sind eventuellen Ausfällen, Insolvenzen oder Preismodelländerungen oft ausgeliefert. Es fehlt meist an Sicherheit, da bei einer Insolvenz oder Einstellung des Softwareprojekts keine Weiterentwicklung garantiert ist. Im Fall von Open Source kann dies durch die Community oder Dienstleister geschehen. Zudem fördert sie die Innovation und hilft zu verhindern, dass eine einzelne Person, Firma oder Organisation die Kontrolle über die Technologie erlangen kann.
- Die Arbeit fokussiert sich außerdem speziell auf die Evaluierung aktueller technischer Aspekte, eine rechtliche Einordnung wird hierbei nicht vorgenommen. Urheberrechtliche Aspekte wie etwa die Gerichtsbeständigkeit werden hier nicht diskutiert, verwiesen sei hierbei etwa auf Mienert et al. (2019, S. 7), die für den PoE-Dienst OriginStamp nachgewiesen haben, dass zwar die Vorgaben hinsichtlich der Integrität eines qualifizierten elektronischen Zeitstempels nach eIDAS-Verordnung eingehalten werden, jedoch die Authentizitätsanforderungen nicht erfüllt sind. Es gibt zur Lösung etwa Vorschläge wie die Einbindung von Notaren (Härer & Fill, 2020, S. 4–5).
- Wie auch schon Leible et al. (2019, S. 19) in ihrer Studie bemerken, ist die Blockchain-Branche schnelllebig und instabil, Projekte können zum Teil auch sehr kurzfristig abgebrochen werden oder verschwinden schlicht, während gleichzeitig wiederum neue hinzukommen. Aus diesem Hintergrund beschränkt sich die Arbeit auf ausgewählte Projekte und Methoden, die seit mindestens 2 Jahren existieren oder von reputablen Wissenschaftsorganisationen begründet wurden.
- Auf die Darstellung der in den Quellen angeführten mathematischen Formeln, Gleichungen und Herleitungen kryptografischer Verfahren wird in dieser Arbeit verzichtet, da für die hier behandelten Aspekte die rein deskriptive Erläuterung ausreicht.

Um herauszufinden, inwiefern PoE-Lösungen auch den zu definierenden Kriterien einer auf offene Wissenschaft ausgelegten technischen Infrastruktur entsprechen, muss zuerst auf die für PoE erforderlichen Grundlagen (grundlegende kryptografische Verfahren, Trusted Timestamping, gewisse Aspekte der Blockchain-Technologie) und das PoE-Verfahren selbst eingegangen, diese in den Kontext eines Open-Science-Ökosystems eingeordnet sowie daraus ein geeigneter Kriterienkatalog aufgestellt werden. In einem späteren Abschnitt werden dann repräsentative PoE-Verfahren vorgestellt und diese schließlich anhand der zuvor erarbeiteten Kriterien verglichen, um daraus eine Handlungsempfehlung sowie ein Fazit abzuleiten.

3 Grundlagen

3.1 Grundlegende kryptografische Verfahren

Die Kryptografie baut wie andere Wissenschaften auf ein Fundament zahlreicher Methoden auf, die über die Zeit immer weiter entwickelt und präzisiert wurden.

Hinsichtlich der Entwicklung hin zu den uns heute zur Verfügung stehenden Verfahren für einen dezentralen und manipulationsgesicherten Existenznachweis auf der Blockchain (Proof of Existence) sind als kryptografische Grundlagen folgende von besonderer Bedeutung:

- Hash-Funktionen, speziell die One-Way-Hashfunktionen (auch kollisionsresistente Einwegfunktionen genannt)
- Digitale Signaturen mit dem Public-Key-Verfahren und Public-Key-Infrastrukturen (PKI)
- Merkle Trees (Hash-Bäume)

3.1.1 One-Way-Hashfunktionen

Hash-Funktionen sind die Basis moderner kryptografischer Verfahren, die heutzutage maßgeblich dazu beitragen, die Schutzziele der Informationssicherheit zu gewährleisten. Hinsichtlich der Daten von Informations- und Kommunikationssystemen garantieren sie nach Semar und Beck (2013, S. 474, 466–467):

- Vertraulichkeit: Die Geheimhaltung der Daten
- Integrität: Die Gewährleistung der Unversehrtheit der Daten
- Authentizität: Die Echtheit der Daten
- Verbindlichkeit: Beweisbarkeit des Ursprungs und Empfangs von Daten

In manchen Fällen auch (Semar & Beck, 2013, S. 467–468):

- Anonymität: Die Nichtspeicherung von personenbezogenen Daten
- Pseudonymisierung: Die Unkenntlichmachung personenbezogener Daten

Die speziellen Eigenschaften von One-Way-Hashfunktionen sind nach Pohlmann (2019, S. 87–88):

- Der Verschlüsselungsalgorithmus ist öffentlich bekannt, sodass die Funktion auch auf jedem System eingesetzt und durch Experten begutachtet werden kann (öffentliche bekannte Einwegfunktion)

- Funktionen dieser Art generieren aus Inhalten beliebiger Länge bzw. Daten beliebiger Größe immer kryptografische Prüfsummen (Hashwerte) in einer fest definierten Länge (eindeutiger „Fingerabdruck“)
- Sie stellen sicher, dass nicht von der generierten Prüfsumme wieder zurück auf den Klartext geschlossen werden kann, daher One-Way-Funktion (Einwegfunktion) genannt
- Die Möglichkeit, aus zwei verschiedenen Inhalten die identische Prüfsumme zu erzeugen, muss rechnerisch ausgeschlossen sein (Kollisionsresistenz)

Unter einer Prüfsumme wird allgemein verstanden „ein aus einem digitalen Objekt (beispielsweise eine Datei oder ein Datensatz) berechneter (Zahlen-)Wert, der dazu dient die Integrität des digitalen Objektes zu kontrollieren“ (Universität Konstanz, 2022). Prüfsummen, im Englischen auch Checksums oder Hashes genannt, werden gebildet, indem der Inhalt, z. B. eines Dokuments, an eine One-Way-Hashfunktion übergeben wird (Pohlmann, 2019, S. 86).

Eine solche Hashfunktion sorgt also dafür, dass sich bei noch so kleinen Änderungen des Inhalts umgehend der Hash verändern würde und allein bei der äußerlichen Betrachtung des Hashes auffällt, dass sich etwas geändert haben muss (Diffusionsprinzip) (Fill & Meier, 2020, S. 6).

Die Kollisionsresistenz verhindert dabei, dass Inhalte unbemerkt manipuliert oder ausgetauscht werden können, ohne dass nach außen nachweislich eine Veränderung der Prüfsumme ersichtlich wäre. Der Hash soll durch seine Länge garantieren, dass nicht gezielt Kollisionen errechnet werden können. Die Stärke eines Hashing-Verfahrens befindet sich jedoch im ständigem Wettlauf mit der zur Verfügung stehenden Rechenleistung, die stetig wächst. Aktuell gelten die Hashfunktionen SHA-3 und SHA-256 als sicher – SHA-1, SHA-2, MD5 und RIPEMD hingegen wurden bereits gebrochen. (Pohlmann, 2019, S. 88.)

3.1.2 Digitale Signaturen mit dem Public-Key-Verfahren (PKI)

Um den durch eine Hashfunktion generierten Fingerabdruck einer Datei, also den Hash, mit einer die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit wahrenden Unterschrift (Signatur) zu versehen (signieren), wird heutzutage gewöhnlich auf eine Kombination mit asymmetrischer Verschlüsselung zurückgegriffen (Semar & Beck, 2013, S. 475.)

Für lange Zeit standen der Kryptografie nur symmetrische Verschlüsselungsverfahren zur Verfügung, bei denen Inhalte mit ein und dem selben Schlüssel ver- und entschlüsselt werden. Das Problem ist hierbei, dass der Schlüsselaustausch auf einem sicheren Kanal passieren muss, da er ansonsten abgehört werden kann. Dieses Problem wurde in den 1970er Jahren gleichzeitig unabhängig voneinander sowohl von Diffie und Hellman als auch von Merkle gelöst, indem sie ein Verfahren erfanden, bei dem zur Verschlüsselung ein anderer Schlüssel genutzt wird als zur Entschlüsselung und nicht von

dem einen auf den anderen geschlossen werden kann. Dieses asymmetrische Verschlüsselungsverfahren wird auch Public-Key-Verfahren genannt.[3] (Semar & Beck, 2013, S. 473.)

Das Verfahren funktioniert grundsätzlich auf folgende Weise (Semar & Beck, 2013, S. 471–473):

- Die Kommunikationsteilnehmer*innen erzeugen sich jeweils ein Schlüsselpaar bestehend aus Public Key und Private Key
- Der Private Key wird geheim gehalten, der Public Key veröffentlicht (etwa auf der eigenen Website oder einem Key Exchange Server)
- Beim Versenden einer Nachricht an die andere Person verschlüsselt die Sender*in diese mit dem Public Key der Empfänger*in
- Die Empfänger*in entschlüsselt den Inhalt mit ihrem Private Key und kann wiederum antworten, indem sie die Antwort mit dem Public Key ihres Gegenübers verschlüsselt und so weiter

Im konventionellen Konzept des Public-Key-Verfahrens tritt entweder eine Zertifizierungsinstanz (eine zentrale Zertifikationsstelle, im Englischen Certification Authority, CA, genannt) hinzu oder es wird ein Web of Trust (Vertrauensnetzwerk von Personen, die sich gegenseitig ihre Schlüssel verifizieren) genutzt, um die Verbindung einer Realwelt-Identität mit einem Schlüssel herzustellen. Eine solche Instanz wird auch Public-Key-Infrastruktur (PKI) genannt. PKIs gelten als vertrauenswürdige Dritte (Trusted Third Party, TTP) und müssen stets sicherstellen, dass sie nicht kompromittiert (angegriffen, manipuliert oder gehackt) werden, weil sonst das Vertrauensnetzwerk zusammenbrechen würde. (Semar & Beck, 2013, S. 475.)

3.1.3 Merkle Trees (Hash-Bäume)

Essenziell für die spätere Entstehung der Blockchain-Technologie und den darauf aufbauenden PoE-Methoden sind ebenso die 1979 von Merkle entwickelten Hash-Bäume (Merkle Trees). Sie sind eine Erweiterung von Hash-Listen und integrieren die oben erläuterten Hashes von Dateien in eine baumartige Struktur, um damit die Integrität ganzer Datenstrukturen verlässlich zu sichern.

Ein solcher Merkle Tree (siehe Abbildung 1) ist folgendermaßen aufgebaut (Fill & Meier, 2020, S. 9):

- Als erstes werden für vorliegende Dokumente (in der Abbildung D_1-D_4) jeweils deren Hashes generiert

3 Es gibt Dokumente, die nahelegen, dass Mitarbeiter des britischen Nachrichtendienstes GCHQ das Verfahren bereits vor den genannten Personen entwickelten. Dies wurde jedoch zu der Zeit nicht öffentlich bekannt gemacht und auch erst durch Aufhebung der Geheimhaltung Jahrzehnte später publik. (Wayner, 1997.) Daher werden hier ihre Arbeiten auch nicht als Bestandteil der (öffentlichen) akademischen Kryptografie erwähnt.

- Die vorliegenden Dokumentenhashes werden paarweise verbunden (konkateniert) und diese Werte auch wieder gehasht (H_1 und H_2)
- Am Ende des Baums wird das Paar der verbliebenen Werte (die Hashes der Datenhashes) miteinander verbunden und daraus ein einziger Wurzelhash H_R, auch Merkle Root genannt, generiert

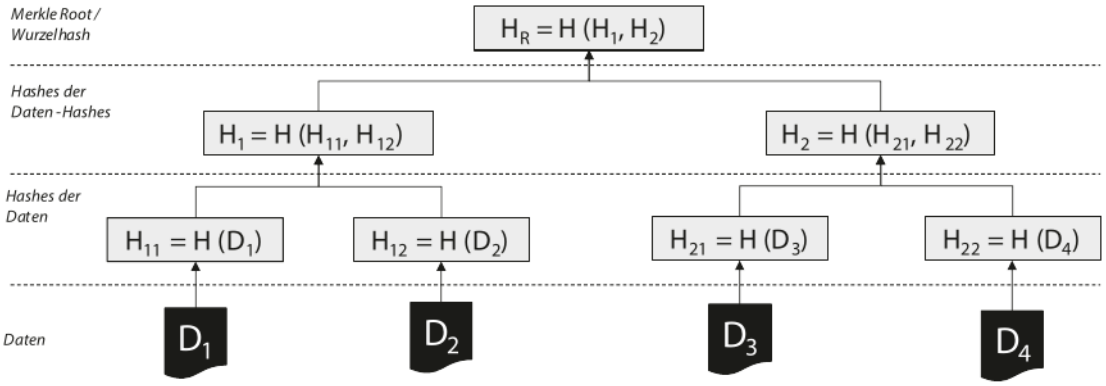


Abbildung 1: Aufbau eines Merkle Trees

Quelle: Fill & Meier, 2020, S. 10

Verbildlicht gesprochen stellt sich der Merkle Tree dar als ein umgedrehter Baum mit Hashwerten als seine Äste und Blätter (unterste Ebene), an dessen Ende (oberster Ebene) der Wurzelhash steht.

Durch den Merkle Tree werden Zero-Knowledge-Proofs möglich, d. h., die Existenz eines bestimmten Dokuments in der Datenstruktur ist nachweisbar, ohne dessen Inhalt zu kennen. Dafür muss nur abgeglichen werden, ob der Hash des zu überprüfenden Dokuments auf der untersten Ebene des Merkle Trees vorhanden ist. Lässt sich mit seinem Nachbar-Hash daraus letztendlich der Merkle Root reproduzieren, ist der Nachweis gesichert erbracht, dass dieses Dokument existiert. (Fill & Meier, 2020, S. 9–11.)

Bei der Überprüfung auf Manipulationen hin reicht es also auch allein den Merkle Root Hash zu kontrollieren, da aufgrund der Verästelung der Hashes in den Ebenen darunter jede einzelne Veränderung, egal an welcher Stelle, eine Änderung des Wurzelhashes zur Folge haben würde.

3.2 Trusted Timestamping

Die Anfänge der manipulationssicheren Zeitstempel (Trusted Timestamping) gehen wie die eben dargestellten kryptografischen Verfahren auch auf eine Zeit weit vor dem Entstehen der Blockchain-Technologie zurück.

Haber und Stornetta widmeten sich 1990 dem aufkommendem Problem, dass digitale Daten einfach verändert werden können und es an Verfahren fehlt, die gesichert nachweisen, wann ein Dokument erstellt und wann es zuletzt geändert wurde. Sie entwi-

ckelten ein digitales Timestamping-Verfahren, dass manipulationssicher ist, gleichzeitig ohne Einsichtnahme in den Inhalt funktioniert und sogar eine Trusted Third Party komplett entbehrlich macht.

Zu der Zeit wurden etwa durch Forschende handschriftlich Labornotizbücher geführt und regelmäßig durch Notar*innen oder Vorgesetzte gegengezeichnet, um im Zweifelsfall neben dem eigentlichen Forschungsresultat auch bei der Anmeldung des geistigen Eigentums die eigene Erfindung belegen zu können. Als Alternative schickten sich Erfinder*innen Nachweise selbst per Post und verwahrten den Umschlag ungeöffnet. Unternehmen führten bei der internen Dokumentation das Vier-Augen-Prinzip ein, um Manipulationen durch Einzelpersonen entgegenzuwirken.

Haber und Stornetta stellen hierbei jedoch zwei Probleme fest:

a) Im Fall von rein digital vorliegenden Daten können Änderungen vorgenommen werden, ohne erkennbar Spuren zu hinterlassen

b) der in den Prozess einbezogenen anderen Instanz (Person oder Partei) muss vertraut werden

(Haber & Stornetta, 1991, S. 438–439.)

Sie folgern daraus, dass es ein digitales Timestamping-Verfahren braucht, das

a) die Integrität und Authentizität eines Dokuments unabhängig vom Medium allein anhand der Daten selbst, also auf den Bit genau, belegen kann

b) kein späteres Einfügen von Zeitstempeln erlaubt

(Haber & Stornetta, 1991, S. 439.)

Das Einsetzen einer Timestamping-Stelle (im Englischen Timestamping Service, TSS)[4], die von den Autor*innen Dokumente in Kopie zugeschickt bekommt, diese mit einem Zeitstempel versieht, anschließend aufbewahrt und bei Bedarf vorhält, halten sie aus folgenden Gründen für bedenkenswert:

a) Die Vertraulichkeit des Inhalts wird untergraben, weil zum einen der Inhalt durch Dritte auf dem Übertragungsweg ausgespäht werden kann und zum anderen so eine unbeteiligte Instanz Zugriff auf die Informationen im Dokument erhält. Hinzu kommt, dass nun auch seitens der TSS Vorkehrungen bezüglich der Dokumentensicherheit getroffen werden müssen

b) Die Übertragung an und die Aufbewahrung bei der TSS braucht zusätzlich Bandbreite und Speicherplatz, die vor allem bei dem Timestamping großer Dokumente zeitaufwendig und teuer werden kann

c) Übertragungsfehler, falsches Timestamping, Datenverlust oder andere Inkompetenzen der TSS könnten zum Verlust des Existenznachweises führen

d) Die TSS führt die Nachweise auf Vertrauensbasis, daher kann sie sich theoretisch mit Autor*innen verabreden, einen gefälschten Zeitstempel zu setzen

4 In der gegenwärtigen Literatur auch oft als Time Stamping Authority (TSA) bezeichnet.

(Haber & Stornetta, 1991, S. 440–441.)

In ihrer Lösung eines TSS gehen sie vorerst von der Vertrauenswürdigkeit der Stelle aus und erweitern das oben beschriebene Konzept um zwei Aspekte:

a) Statt dem Dokument selbst wird der TSS ein Hash des Dokuments übermittelt, der von der Stelle mit einem Zeitstempel versehen wird. Dabei wird ein Hashing-Verfahren gewählt, das Kollisionen möglichst unwahrscheinlich hält (kollisionsresistent) und in eine Richtung (one-way) funktioniert. Dies löst die Probleme mit der Übertragung und Aufbewahrung des Dokuments und exponiert nicht dessen Inhalt.

b) Die TSS versieht den erhaltenen Dokumentenhash nicht nur mit einem Zeitstempel, sondern auch mit einer digitalen Signatur und schickt diesen zurück an die Autor*innen, die nun den Hash, den korrekten Eingang sowie die Zeitangabe gegenprüfen können. Etwaige Risiken durch Fehler auf der Seite der TSS sind so ausgeschlossen und die Buchführung seitens der TSS wird auf ein Minimum reduziert.

(Haber & Stornetta, 1991, S. 441–443.)

Für das verbleibende Vertrauensproblem skizzieren sie zwei Lösungsmöglichkeiten:

a) Jedes ausgegebene Zertifikat wird neben Zeitstempel, Dokumentenhash und Signatur zusätzlich mit einer den Autor*innen zugeordneten einzigartigen ID versehen, sequenziell nummeriert und mit dem Hash des vorhergehenden Zertifikationsprozesses verkettet (Linking Scheme). Autor*innen können so vorangegangene als auch kommende Zertifikate zur Validierung ihres eigenen Zertifikats nutzen. Rück- oder Vordatierungen seitens der TSS wären so nur noch möglich, wenn die gesamte Kette der ausgestellten Zertifikate gefälscht wird bzw. in solch einer Länge, dass sich eine etwaige Prüfinstanz dadurch täuschen lässt.

b) Mittels einem PRNG (Pseudo Random Generator) und dem Dokumentenhash als Seed (Startwert) werden aus einem Pool von einzigartigen IDs vorangegangener Autor*innen zufällig eine bestimmte Anzahl ausgewählt und diese signieren dann den aktuell vorliegenden Dokumentenhash (Distributed Trust Scheme). Eine Verabredung zur Fälschung wird durch die Zufallswahl der signierenden Teilnehmer*innen minimiert. Obwohl es eine Form von Verzeichnis der IDs (dem Pool) geben muss, ist dieser Ansatz auch losgelöst von einer zentralen Timestamping-Instanz wie der TSS, also dezentral, umsetzbar.

(Haber & Stornetta, 1991, S. 444–447.)

3.3 Blockchain-basiertes Trusted Timestamping

Die im vorherigen Abschnitt dargestellten Ansätze von Haber und Stornetta werden heutzutage als Wegbereiter der Blockchain-Technologie aufgefasst. Nicht zuletzt, weil sich das Bitcoin begründende Whitepaper von Satoshi Nakamoto (2008) mit drei von insgesamt acht Zitationen auf diese Arbeiten von Haber und Stornetta bezieht.

Entsprechend bezeichnet*nen Nakamoto (2008) seine*ihre[5] Lösung des Double-Spending-Problems[6], die in das weltweit erste von einer Mittelsperson (Trusted Third Party) unabhängige dezentrale digitale Transaktionssystem mündete, auch als „peer-to-peer distributed timestamp server“ (S. 1).

In den folgenden Abschnitten wird zuerst die Blockchain-Technologie im Lichte der darauf aufbauenden Proof-of-Existence-Methoden betrachtet, dazu wird eingegangen auf die grundlegenden Voraussetzungen:

- Merkle Trees in einer Kette von Datenblöcken
- Dezentrale Public-Key-Intrastrukturen (DPKI)
- Konsensmechanismen
- Governance-Modelle
- Smart Contracts

Schließlich wird in einem eigenen Abschnitt die PoE-Methode definiert sowie ihre Eigenschaften und Grenzen aufgezeigt.

Blockchains lassen sich eingangs definieren als „verteilte elektronische Register, die mithilfe kryptografischer Verfahren und Konsensalgorithmen vor Manipulationen geschützt sind“, „als vertrauenswürdige Quelle von Informationen dienen“ und „dabei auf eine zentrale Überwachungsinstanz verzichte[n]“ (Fill & Meier, 2020, S. 1–2). Mit verteiltem Register (Distributed Ledger[7]) ist die Datenstruktur für eine dezentrale Buchführung gemeint. Der Konsens (Konsensmechanismus, Consensus mechanism) löst das byzantinische Problem[8] und dient daher der Betrugsprävention. (Fill & Meier, 2020, S. 1–3.)

Die derzeit beiden größten Blockchains der Welt sind das Bitcoin-Netzwerk[9] und Ethereum. Das Bitcoin-Netzwerk wurde 2009 als erste Internet-basierte Blockchain in Betrieb genommen[10] und ist bis heute die weltweit größte ihrer Art[11]. Ethereum ist nach

5 Die Identität von Satoshi Nakamoto ist nicht öffentlich bekannt, daher kann auch nicht ausgeschlossen werden, dass es sich um eine Gruppe handelt.

6 Das Verhindern, dass die eine und selbe veräußerte digitale Geldeinheit doppelt ausgegeben werden kann.

7 Daher gehören Blockchains auch zu den Distributed-Ledger-Technologien (DLT).

8 Das Korrumpieren eines Netzwerks durch die Lieferung fehlerhafter oder falscher Daten seitens einzelner Knoten.

9 In dieser Arbeit wird explizit vom Bitcoin-Netzwerk gesprochen, um eine Gleichsetzung des Blockchain-Netzwerks mit den auf der Blockchain transferierten Werteinheiten Bitcoin (BTC) zu vermeiden.

10 Der erste Bitcoin-Block („Genesis-Block“) wurde am 03.01.2009 erschaffen (Blockchain.com, 2009).

11 Das Bitcoin-Netzwerk hat aktuell über 15.000 aktive Knoten, auf denen die Blockchain redundant gespeichert und zur Verfügung gestellt wird (Coin Dance, 2022), und eine Marktkapitalisierung von über 300 Milliarden US-Dollar (CoinGecko, 2022a).

Bitcoin das weltweit zweitgrößte Blockchain-Projekt[12], was nicht zuletzt an seiner Smart-Contract-Funktionalität (siehe weiter unten) liegt, und wird seit 2015 betrieben[13].

3.3.1 Merkle Trees in einer Kette von Datenblöcken

Die Blockchain-Technologie bedient sich der Merkle-Tree-Methode (siehe oben) und setzt diese bei der Verkettung einzelner aufeinander aufbauenden Datenblöcke ein, woraus die namensgebende Kette von Blöcken (Blockchain) entsteht.

Das Prinzip der Formierung einer Blockchain-Datenstruktur (siehe Abbildung 2) sei kurz erläutert anhand zwei gegebener Blöcke (Fill & Meier, 2020, S. 18–19, 24):

- Der Block 1 besteht aus zwei Transaktionen T_1 und T_2, woraus die Hashes H_1 und H_2 generiert wurden. Aus den beiden Hashes H_1 und H_2 wurde nach dem Merkle-Prinzip der Wurzelhash H_{12} erzeugt. Der Merkle Root H_{12} ist dann wiederum im Header des Blocks 1 BH_1 hinterlegt
- Der nachfolgende Block 2 umfasst die Transaktionen T_3 und T_4, woraus nach dem selben Prinzip letztendlich der Merkle Root H_{34} in den Blockheader dieses Blocks geschrieben wird. Der Block 2 enthält jedoch im Header zusätzlich eine Referenz auf den Block Header 1 BH_1 und übernimmt damit die Funktion des führenden Blocks der Blockchain, bevor ein weiterer Block folgt, der Transaktionen in sich aufnimmt
- Nachfolgende Blöcke inkorporieren dann in der selben Weise immer Referenzen auf den jeweiligen Header des vorangegangen Blocks

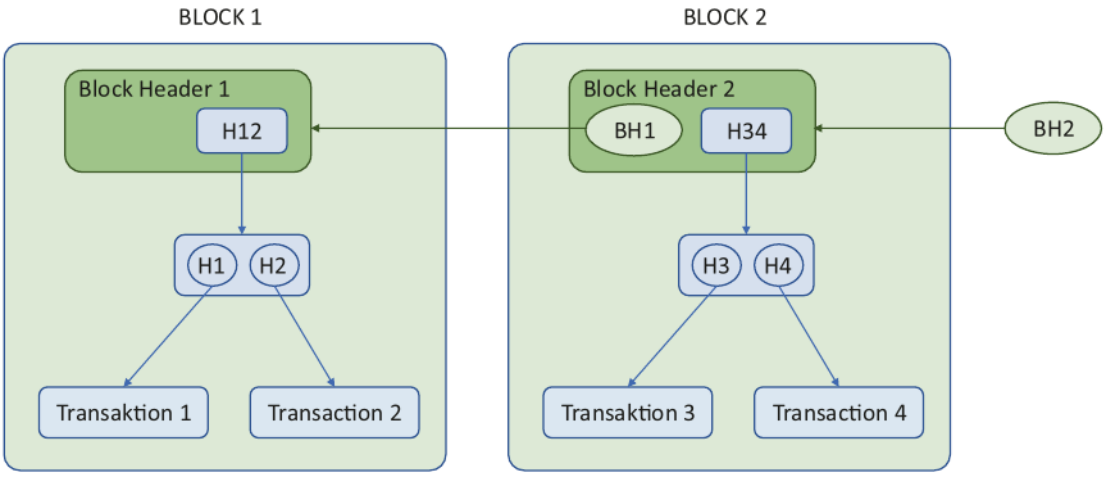


Abbildung 2: Formierung einer Blockchain-Datenstruktur

Quelle: Fill & Meier, 2020, S. 19

12 Ethereum verfügt aktuell über 2300 aktive Knoten (Etherscan, 2022) und eine Marktkapitalisierung von über 130 Milliarden US-Dollar (CoinGecko, 2022b).

13 Der Genesis-Block von Ethereum wurde am 30.07.2015 initiiert (Etherscan, 2015).

Der Header eines Blocks enthält im Wesentlichen, hier am repräsentativen Beispiel der Bitcoin-Blockchain (Fill & Meier, 2020, S. 23):

- Protokollversion
- Referenz: Der oben beschriebene Verweis auf den vorherigen Block in der Kette
- Zeitstempel: Zeitpunkt der Erstellung des Blocks
- Target: Zahl zur Aushandlung des Schwierigkeitsgrads (Difficulty), um den Block zu erzeugen
- Nonce (Number used once): Eine Zufallszahl, die ebenfalls zur Erzeugung des Blocks erforderlich ist
- Merkle Tree

Durch die beschriebene Datenstruktur garantiert die Blockchain eine fortwährende Integrität aller enthaltenen Daten, da Änderungen in einzelnen Blöcken immer Auswirkungen auf die gesamte Kette haben würden: Hashes müssten neu berechnet, die Hashbäume und Block-Header diese Hashwertänderungen adaptieren. Mit dem Hinzukommen eines jeden neuen Blocks prüft eine Blockchain also entsprechend die Gesamtheit aller in ihr enthaltenen Hash-Referenzen auf deren Konsistenz und Korrektheit. Fill & Meier (2020, S. 20–22) sprechen dabei von einem „Alles-oder-Nichts-Prinzip“: „Wird eine Änderung in der Blockchain-Datenstruktur irgendwo vorgenommen, so folgt eine Kaskade von Änderungen ab dieser Stelle bis hin zum Kopf der Kette oder es wird überhaupt keine Änderung in der Kette erwirkt“.

3.3.2 Dezentrale Public-Key-Intrastrukturen (DPKI)

Integrität, Authentizität und Verbindlichkeit bzw. Anonymität oder Pseudonymität werden bei einer Blockchain durch den Einsatz der Public-Key-Methode gewährleistet (Fill & Meier, 2020, S. 17). Dies hatte*n bereits Nakamoto (2008) im Bitcoin-Whitepaper hinsichtlich der Durchführung von Transaktionen postuliert: „We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin“ (S. 2).

Das Schutzziel der Verfügbarkeit wird erreicht durch die redundante Speicherung der Blockchain auf einem verteilten Netzwerk (P2P-Netzwerk) ohne zentrale Instanz (TTP). Insgesamt entsteht dadurch eine manipulationssichere dezentrale PKI, auf der Transaktionen getätigt werden.

Die Vertraulichkeit ist nur in Bezug auf die Identitäten der Sender*innen und Empfänger*innen gegeben, die Transaktionen an sich sind öffentlich durch jede*n auf der Blockchain einsehbar und nachverfolgbar[14].

14 Es gibt inzwischen auch spezielle Blockchain-Protokolle, die durch verschiedene Mechanismen eine Verschleierung der geschehenen Transaktionen erreichen. Auf diese wird hier aufgrund der fehlenden Relevanz für die Themensetzung dieser Arbeit nicht eingegangen.

3.3.3 Konsensmechanismen

Um die Integrität des Blockchain-Netzwerks sicherzustellen, also dass dieses nicht etwa von böswilligen Akteur*innen übernommen werden kann, die Transaktionen zu ihren Gunsten manipulieren, wurde der Konsensmechanismus geschaffen.

Konsens meint im Kontext der Blockchain-Technologie die Einigung unter den am Netzwerk beteiligten Knoten, inwiefern ein nächster Block der Kette hinzugefügt werden darf (Ramamurthy, 2020, S. 296).

Im Fall von Bitcoin wurde dabei das Proof-of-Work-Konzept (PoW) aufgegriffen, das den Konsens auf Basis der Rechenleistung aushandelt: Die Entscheidung der Mehrheit findet seine Repräsentation in der längsten Kette, in die am meisten PoW-Leistung investiert wurde. Wenn die Mehrheit an Rechenleistung durch gutwillige Knoten gestellt wird, fällt die Kette eines Angreifenden zurück, weil dieser ab dem kompromittierten Block alle Folgeblöcke neu berechnen muss und irgendwann nicht mehr aufholen kann. (Nakamoto, 2008, S. 3). (Nakamoto, 2008, S. 3.)

Satoshi Nakamoto (2008, S. 6–8) wies*en damals in seinem*ihren*ihrem Konzeptpapier nach, dass die Wahrscheinlichkeit, mit einer Alternativkette aufholen zu können, exponentiell abnimmt, umso mehr Blöcke in der Zeit hinzukommen.

In der Praxis funktioniert die Konsensbildung bzw. Transaktionsabwicklung in einem Blockchain-Netzwerk folgendermaßen (Ramamurthy, 2020, S. 297):

- Die zu verarbeitenden Transaktionen werden unter Entrichtung einer Transaktionsgebühr durch die Sender*innen in das Blockchain-Netzwerk eingespeist, also angekündigt
- Die Transaktionen werden durch bestimmte Arbeitsknoten (Miner) auf Konsistenz geprüft
- Gültige Transaktionen landen in einem Pool unbestätigter Transaktionen (Mempool), ungültige Transaktionen werden abgewiesen
- Die Miner formen Transaktionen zu einem Block
- Im Fall eines PoW-Konsensmechanismuses:
    - Die Miner rechnen um die Wette, indem sie ein kryptografisches Puzzle lösen
    - Der erste Miner, der das Puzzle löst, darf den Block an die Kette hängen und erhält zudem eine Belohnung (Block Reward) sowie die in dem Block entrichteten Transaktionsgebühren
- Die anderen Knoten verifizieren den geschaffenen Block und bestätigen damit die enthaltenen Transaktionen
- Nach einer gewissen Anzahl von Bestätigungen des Blocks können die Transaktionen als gesichert bestätigt gelten

Inzwischen haben sich im Blockchain-Bereich neben PoW noch zwei weitere Konsensmechanismen herausgebildet, die für die weitere Abhandlung besonders relevant sind:

- Proof of Stake (PoS): Die Knoten mit den meisten Werteinheiten (Crypto-Coins oder Tokens) im Besitz, auch Validatorknoten genannt, entscheiden nach einem Rundlauf-Verfahren (Round-Robin-Verfahren) über das Hinzukommen neuer Blöcke. Dahinter steht die Annahme, dass Knoten mit dem größten Vermögen (Stake) wenig Anreiz darin sehen, das Netzwerk zu destabilisieren. Die Transaktionskosten gehen an den Validatorknoten, der anstatt des Miners im PoW-Konsensalgorithmus hier den Block mintet. (Ramamurthy, 2020, S. 297.)
- Proof of Authority (PoA): Es werden eine gewisse Anzahl an Autoritäten bestimmt, die als Validatorknoten allein Blöcke an die Blockchain anhängen dürfen. Die Vergabe der Validator-Eigenschaft wird durch eine zentrale Instanz vorgenommen, die geeignete Autoritäten anhand bestimmter Kriterien (etwa Offenlegung der eigenen Identität, Vertrauenswürdigkeit, Reputation) aussucht und dann vorab als validierende Knoten festlegt. Der PoA-Konsensmechanismus stellt damit das Konzept der Dezentralisierung der Blockchain in Frage. (Schiller, 2022b.)

3.3.4 Governance-Modelle

Im Zusammenspiel mit dem Konsensmechanismus nimmt auch noch das Governance-Modell eine wichtige Rolle ein. Für PoE-Dienste ist dabei die Zugänglichkeit von Relevanz, also inwiefern die Teilnahme am Netzwerk möglich ist. Allgemein lassen sich dabei Blockchans in öffentlich (permissionless) und privat (permissioned) einteilen.

An Blockchains, die permissionless („zulassungslos“ oder „genehmigungsfrei“) sind, kann jede*r im vollen Umfang teilnehmen. Das prominenteste Beispiel dafür ist das Bitcoin-Netzwerk, zu dessen fundamentalen Prinzipien die Permissionlessness zählt: „No arbitrary gatekeepers should ever prevent anybody from being part of the network (user, node, miner, etc)“ (Bitcoin Wiki, 2017). Diese Herangehensweise hat seine Wurzeln in dem Grundsatz, keiner am Netzwerk teilnehmenden Instanz zu vertrauen und allein im Aushandeln des Konsens unter allen Instanzen die Sicherheit gewahrt bleibt, dass von niemandem nachträglich Veränderungen an der Blockchain vorgenommen werden können. Entsprechend setzen Kryptogeldsysteme, die unabhängig von Dritten sein wollen, auf dieses Modell. Hierbei wird auch von einem trustless Network („vertrauenslosem Netzwerk“) gesprochen. (Raj, 2019, S. 15–16.)

Permissioned („zulassungsbeschränkte“ oder „genehmigungsbasierte“) Blockchains sind gegenüber Teilnehmenden restriktiv, sie knüpfen die Teilnahme selbst und auch entsprechende Nutzungsberechtigungen an bestimmte Voraussetzungen. Neuzugänge bekommen von einer Zulassungsinstanz, etwa einem*einer Administator*in, ihre Rollen zugewiesen. Diese Art von Blockchain-Netzwerke sind oft aus ganz individuellen Anwendungsfällen heraus entstanden, die eine Beschränkung auf einen bestimmten Kreis von Nutzer*innen bedingen. Im Kontrast zu einer permissionless Blockchain kann im Fall der permissioned Blockchain von einem Trust Network („Vertrauensnetzwerk“) ge-

sprochen werden. (Raj, 2019, S. 16.) Ein Beispiel hierfür ist die bereits erwähnte Bloxberg-Blockchain, die aus dem Bedarf der Scientific Community nach einem dezentralen Netzwerk entstanden ist.

Nach der Typologie von Raj (2019, S. 17) ließe sich Bloxberg aber auch als konsortiale Blockchain einordnen. Darunter ist eine permissioned Blockchain zu verstehen, bei der die Ausführung der Prozesse auf der Blockchain auf mehrere Knoten verteilt ist, die durch unterschiedliche Organisationen betrieben werden. Im Falle von Bloxberg handelt es sich dabei um ein Konsortium von Forschungsorganisationen und -einrichtungen. Die konsortiale Blockchain wird weiter als ein semi-dezentralisiertes Hybrid-Modell beschrieben, das Aspekte einer permissioned Blockchain mit einer gewissen Permissionlessness zu vereinen versucht. Ob das zutrifft und was solch ein Modell im Einzelnen für Auswirkungen hat, wird in der späteren Evaluation noch zu untersuchen sein.

3.3.5 Smart Contracts

Das Ethereum-Projekt läutet bei dem Launch 2015 mit seiner Implementierung von Smart Contracts eine neue Stufe in der Entwicklungsgeschichte der Blockchain-Technologie ein. Nicht nur Wertetransaktionen können durchgeführt werden, sondern ganze Coderoutinen lassen sich Turing-vollständig in eine durchgängig betriebene, unveränderbare virtuelle Maschine (Ethereum Virtual Machine, EVM) schreiben, die durch das Blockchain-Netzwerk von Knoten repräsentiert wird (Buterin, 2014, S. 1).

Smart Contracts sind im diesem Sinne nicht zu verstehen als die Abbildung von herkömmlichen Verträgen auf der Blockchain, sondern „they are more like 'autonomous agents' that live inside of the Ethereum execution environment, always executing a specific piece of code when 'poked' by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables“ (Ethereum.org, 2022a, Abschn. „Ethereum Accounts“).

Seither lassen sich native dezentrale Applikationen (dApps) implementieren, also Programme, die nicht nur mit einer Blockchain interagieren, sondern auf ihr selbst ausgeführt werden. Neben vielen anderen Anwendungsfällen kommen Smart Contracts auch in neueren PoE-Konzepten zum Einsatz (Shawn et al., 2021). Smart Contracts können jedoch nicht nur dApps, sondern auch die grundlegenden Abläufe der Blockchain definieren. Etwa sind im Fall der Bloxberg-Blockchain der Konsensmechanismus sowie Governance-Funktionalitäten im Genesis als Smart Contracts angelegt (Kleinfercher et al., 2020, S. 13).

3.3.6 Proof of Existence (PoE)

Proof-of-Existence-Verfahren vereinen nun die Timestamping-Funktionalität auf der Blockchain mit dem Hashing von Dateien. Indem eine One-Way-Hashfunktion auf ein zu attestierendes Dokument angewandt wird, entsteht ein einzigartiger Identifikator über den Inhalt des Dokuments. Die Authentizität des Dokuments lässt sich sodann immer wieder erneut verifizieren, indem der selbe Hashing-Algorithmus auf die Datei an-

gewandt wird. Deckt sich die alte mit der neu generierten Prüfsumme, wurden am Dokument keine Änderungen vorgenommen. Die Prüfsumme wird mittels einer Transaktion in der Blockchain verankert, wodurch diese zur Dokumentenregistratur wird. (Swan, 2015, S. 37.) Analog zum Trusted Timestamping Service (TSS) ist also auch hier kein Bruch der Vertraulichkeit erforderlich, weil nur der Hash und nicht die Datei auf der Blockchain gespeichert ist.

Somit lässt sich Proof of Existence allgemein definieren als ein auf der Blockchain verzeichneter Nachweis über die Existenz eines exakten Dateninhalts zu einem bestimmten Zeitpunkt, ohne den Inhalt selbst zu offenbaren (Swan, 2015, S. 37–38).

In der Bitcoin-Community wurde die PoE-Methode in der Vergangenheit auch als Proof of Publication bezeichnet und darauf hingewiesen, dass Jeremy Clark und Aleksander Essex 2012 den ersten Ansatz einer solchen Methode in ihrem Paper „CommitCoin: Carbon Dating Commitments with Bitcoin“ dargelegt haben (Bitcoin Wiki, 2014).

3.3.6.1 PoE-Dienste

Das PoE-Verfahren wird aktuell von verschiedenen kommerziellen und nicht-kommerziellen Anbietern (auch als Blockchain Attestation Services bezeichnet) angeboten. Die Angebote umfassen oft ein ganzes Paket von Dienstleistungen: das Verzeichnen, Speichern und Attestieren von Dokumenten, Validierungs- und Notariatsdienste als auch den Urheberrechtsschutz (Intellectual Property, IP). (Swan, 2015, S. 38.)

Ein bekanntes, inzwischen kommerziell-ausgerichtetes, Beispiel, das bis heute existiert und als Attestation Service u. a. auch für wissenschaftliche Publikationen auf der Bitcoin-Blockchain begonnen hat (Gipp et al., 2015, S. 2), ist OriginStamp[15].

Ein dezidierter PoE-Dienst für Forschungsoutput, der momentan Open Source und kostenfrei ist, steht seit 2020 mit dem Research Data Certification Service auf der Bloxberg-Blockchain bereit[16].

Neben den eben genannten bereits aktiven public Blockchains, die permissionless oder permissioned einen PoE-Service bieten, gibt es auch die sogenannten BaaS-Lösungen (Blockchain-as-a-Service), die von vielen großen Cloud-Anbietern bezogen werden können (Schiller, 2022a). Über BaaS kann mit wenig Aufwand eine eigene Blockchain in Betrieb genommen werden (Blockchain aus der Cloud), auf dieser sich dann wiederum ein PoE-Dienst implementieren oder aufsetzen ließe. Das Open-Source-Blockchain-Projekt Hyperledger, auf dessen Frameworks viele der kommerziellen BaaS-Lösungen basieren, bietet mit seinen offenen Code-Repositorien aber auch die Möglichkeit, eine Blockchain eigenständig auf eigenen Servern aufzusetzen.

15 https://originstamp.com

16 https://certify.bloxberg.org

3.3.6.2 Funktionsweise von PoE-Diensten

Am Beispiel eines der ältesten Anbieter mit dem die Methode prägenden Namen Proof of Existence[17] soll kurz die Grundfunktionalität eines PoE-Dienstes skizziert werden (Swan, 2015, S. 39):

- Auf einer Website wird ein spezielles Dateiformular mit eingebautem Hash-Algorithmus bereit gestellt, das lokal im Browser aus der gewünschten Datei eine Prüfsumme generiert, ohne den Inhalt online zu übertragen
- Der generierte Dokumentenhash wird sodann in eine Blockchain-Transaktion eingebettet (siehe Abbildung 3)
- Sobald die Transaktion durch die zuständigen Knoten in einem Block erfasst und an die Blockchain angehängt wurde, gilt der Zeitstempel des Blocks als attestierter Zeitstempel des Dokuments und der Dokumenteninhalt in Form der Prüfsumme als fest in die Blockchain verankert
- Der Dokumentenhash ist fortan der permanente Marker, der auf der Blockchain einsehbar ist und zur Verifizierung auch lokal durch das Anwenden des Hashingprozesses auf das Originaldokument reproduziert werden kann

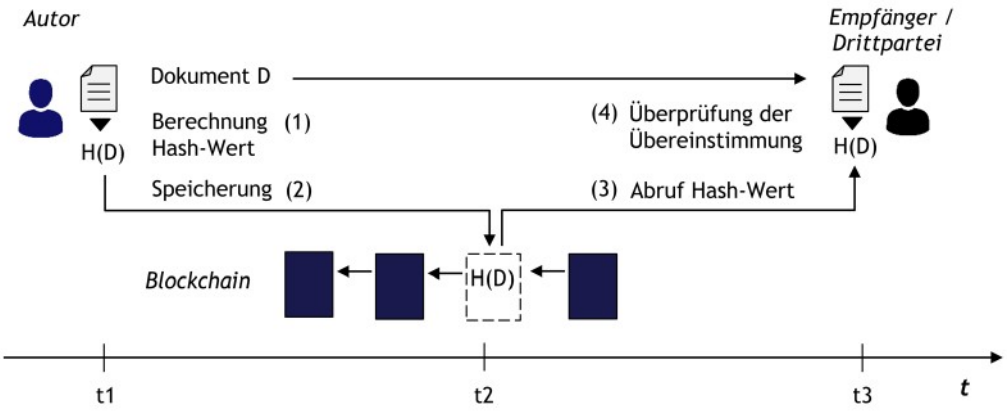


Abbildung 3: Prinzip der Blockchain-basierten Attestierung von Dokumenten

Quelle: Härer & Fill, 2020. S. 2

Die Person, die einen solchen Dokumentenhash in einer Blockchain verankert oder dies in Auftrag gegeben hat, kann so zu einem späteren Zeitpunkt beweisen, dass sie zu dem in der Blockchain verzeichneten Zeitpunkt im Besitz des Dokuments war (Swan, 2015, S. 39). In der Praxis wird den Nutzer*innen zu diesem Zweck meist am Ende des Prozesses eine Attestierungsdatei ausgegeben (siehe Abbildung 4). Diese kann technisch unterschiedlich umgesetzt sein (im abgebildeten Beispiel etwa eine .ots Attestierungsdatei des Bitcoin-basierten PoE-Dienstes OpenTimestamps), sie enthält jedoch die für eine künftige Verifizierung erforderlichen Informationen, für gewöhnlich

17 https://proofofexistence.com

mindestens den Dokumentenhash und die damit assoziierten Blockchain-Hashes. Die Datei kann später einer Drittpartei auch mitsamt des Dokuments übergeben werden, sodass diese selbst für sich die bereits geschehene Attestierung des Dokuments zu dem in der Vergangenheit liegenden Zeitpunkt aus den in der Blockchain verzeichneten Daten heraus rekonstruieren kann. (Härer & Fill, 2020, S. 3.)

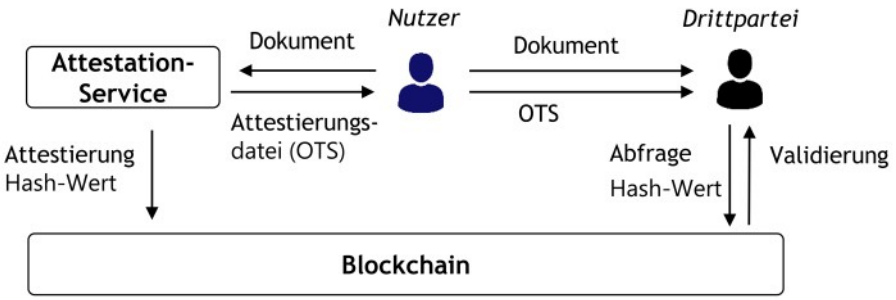


Abbildung 4: Attestierung unter Nutzung eines Attestation-Services

Quelle: Härer & Fill, 2020. S. 3

Üblicherweise werden von vielen PoE-Diensten die Hashes mehrerer Dokumente in einer Transaktion zusammengefasst (etwa jene aller Nutzer*innen des Dienstes in dem jeweiligen Moment oder eines bestimmten Zeitraums) auf die Blockchain geschrieben. Die einzelnen Dateichecksummen sind dabei oft in einem Merkle Tree organisiert. So lassen sich einzelne Hashs allein aus dem Merkle Root (Top-Hash) herleiten, was deutlich effizienter ist. (Härer & Fill, 2020, S. 3; Mienert et al., 2019, S. 2–3.)

3.3.6.3 Voraussetzungen und Grenzen von PoE

PoE-Methoden setzen zwei Gegebenheiten grundlegend voraus (Swan, 2015, S. 39):

- Die mit der Attestation assoziierten Private Keys dürfen nicht verloren werden
- Die genutzte Blockchain muss auch noch zu einem späteren Zeitpunkt verfügbar sein

Es müssen daher Sicherungs- und Sicherheitsvorkehrungen bei der Schlüsselaufbewahrung getroffen werden und es ist ratsam, eine Blockchain zu wählen, die beständig ist. Beständigkeit kann als allgemein gegeben erachtet werden, wenn die Blockchain auf einer offenen Codebasis beruht, die von einer aktiven Entwickler*innen-Community betreut wird. Swan (2015, S. 39) merkt dazu an, aus diesem Grund eine gängige Blockchain wie das Bitcoin-Netzwerk zu nutzen.

Das PoE-Verfahren unterliegt auch gewissen Einschränkungen, die bei der folgenden Auseinandersetzung noch zu berücksichtigen sind (Swan, 2015, S. 39–40):

- Es fallen gewöhnlicherweise Kosten für die auf der Blockchain getätigten Transaktionen an, während andere TTP-basierte Trusted-Timestamping-Dienste oftmals in einem gewissen Umfang kostenlos nutzbar sind

- Das erforderliche Bestätigen einer Transaktion durch die Knoten des Blockchain-Netzwerks (siehe Konsensmechanismus oben) erzeugt einen Zeitverzug, sodass der Zeitpunkt der Blockerstellung von dem Zeitpunkt abweichen kann, an dem das Dokument ursprünglich eingereicht wurde. Das Setzen eines möglichst präzisen Zeitstempels gestaltet sich also schwierig.
- PoE weist nicht den aktuellen Besitzstatus eines Dokuments nach, also dient nicht als Proof of Ownership

Proof of Ownership ist eine Methode, um die verschiedenen Besitzer*innen einer bestimmten Information über den Verlauf der Zeit nachzuverfolgen (Bitcoin Wiki, 2015; Raj, 2019, S. 170–171). Durch das Aufkommen von NFTs (Non-Fungible Tokens) im Zusammenhang mit bestimmten Token-Standards auf der Ethereum-Blockchain ist das Interesse an solchen Methoden in den letzten Jahren enorm gestiegen. Für die vorliegende Arbeit ist aber vielmehr der Nachweis über die Existenz eines Inhalts der initialen Erzeuger*in von Relevanz und nicht die Historie der Besitzer*innen, daher wird dieser Themenkomplex hier nicht behandelt.

3.3.6.4 Notwendigkeit einer Blockchain

Auch wenn in der vergangenen Zeit das Thema Blockchain immer wieder in vielen verschiedenen Zusammenhängen diskutiert wird (siehe Einführungskapitel), zeigt etwa eine repräsentative Studie des Bitkom, dass in der Praxis die Blockchain-Technologie bisher nur von den wenigsten Unternehmen in Deutschland wirklich eingesetzt wird, auch weil es an belastbaren Anwendungsfällen fehlt (Streim & Faupel, 2021).

An dieser Stelle muss sich also auch bei dem Anwendungsfall, den diese Arbeit behandelt, die Frage gestellt werden, ob für diesen der Einsatz einer Blockchain sinnvoll sein kann.

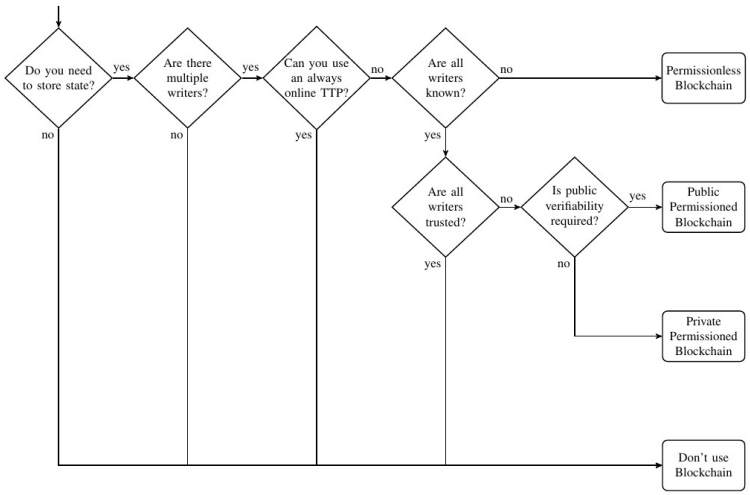


Abbildung 5: Flowchart zur Einschätzung der Notwendigkeit einer Blockchain

Quelle: Wüst & Gervais, 2018, S. 47

Ein Werkzeug, um dieser Frage nachzugehen, liefern Wüst und Gervais (2018) mit ihrem Flowchart (siehe Abbildung 5).

Mit dessen Hilfe kann anhand einiger weniger Fragen eingeschätzt werden, für welche Anwendungsfälle sich eher eine Blockchain oder eine konventionelle zentrale Datenbank eignet. Bei beiden möglichen Pfaden, die im Fall von Existenznachweisen eingeschlagen werden können (siehe Tabelle 1), läuft es auf die Nutzung der Blockchain-Technologie hinaus. Insofern alle Entitäten mit Schreibrechten bekannt sind, würde eine öffentliche permissioned Blockchain in Frage kommen, andernfalls eine permissionless Blockchain.

Tabelle 1: Notwendigkeit einer Blockchain für Existenznachweise

Frage	**Antwort**
Müssen Zustände gespeichert werden?	Ja, es müssen dauerhafte Nachweise über die Existenz von Dokumenten und Daten gespeichert werden.
Gibt es mehrere Entitäten, die Daten schreiben müssen?	Ja, innerhalb der Scientific Community, Wissenschaftsgemeinschaften und selbst einzelnen Forschungseinrichtungen sind es zahlreiche Entitäten, die ihre Existenznachweise unabhängig voneinander verzeichnen wollen.
Kann auf eine ständig online verfügbare TTP zurückgegriffen werden?	Nein, wie im Abschnitt zu Trusted Timestamping ausgeführt, kann im Kontext von Existenznachweisen generell keiner Trusted Third Party vertraut werden.
Sind alle Entitäten mit Schreibrechten bekannt?	Im globalen Rahmen der gesamten Scientific Community wäre dies mit Nein zu beantworten. In kleineren Zusammenhängen wie Forschungsgemeinschaften oder einzelnen Forschungsinstituten wäre dies möglicherweise mit Ja zu beantworten.
Ist allen Entitäten mit Schreibrechten zu trauen?	Nein, hier sei ebenfalls auf die Argumentation im Abschnitt zu Trusted Timestamping verwiesen, dass im Kontext von Existenznachweisen idealerweise so wenig Vertrauen wie möglich angebracht ist.
Ist eine öffentliche Verifizierbarkeit erforderlich?	Ja, der Nachweis über die Existenz eines Dokuments oder von Daten muss öffentlich verifizierbar sein, nur dies gewährleistet eine unabhängige Prüfung durch Dritte im Kontext einer offenen Wissenschaft (siehe Abschnitt zu Open Science unten).

Wüst und Gervais kommen in ihrer dazugehörigen Fallstudie hinsichtlich dem Schutz des geistigen Eigentums zu dem Schluss, dass sich für diesen Zweck zwar auch eine

TTP wie etwa das Patentamt eigenen würde, PoE-Dienste aber den Prozess vereinfachen und keine Offenlegung der Inhalte erfordern (Wüst & Gervais, 2018, S. 52).

3.3.6.5 PoE-relevante Normen in Deutschland

Seit 2015 sind in Deutschland die sogenannten „Systeme zur Beweiswerterhaltung kryptografisch signierter Dokumente“ nach DIN 31647 genormt. Diese Norm basiert auf dem in der digitalen Langzeitarchivierung gängigen OAIS-Standard (Open Archival Information System) nach ISO 14721:2012 und DIN 31644. Sie soll dabei Anwendung finden „auf alle elektronischen Dokumente/Daten, deren durch kryptographische Elemente erzeugter Beweiswert[18] erhalten werden soll“. (DIN 31647, 2015, S. 6.)

Konkret werden dem nach OAI definierten Archivpaket (AIP, Archive Information Package) zum Zweck der Beweiserhaltung in den Fixity-Informationen[19] ein Satz von Beweisdaten und beweisrelevanten Daten beigegeben, die mittels einer Beweisdatenbeschreibung einem enthaltenen digitalen Objekt zugeordnet sind. Solche Erzeugnisse bezeichnet die Norm als „Archivpakete mit kryptografischen Beweismitteln“. (DIN 31647, 2015, S. 22–23.) Während auf der Blockchain der Merkle Root als maßgeblicher Identifikator zum Abruf eines Blocks, in dem letztendlich Dokumentenhashes hinterlegt sind, gilt, ist es hier der Archivdatenobjektidentifikator, der den Abruf eines AIP mit den Beweisdaten ermöglicht (DIN 31647, 2015, S. 19). Angemerkt sei hierbei, dass die gängigen Implementierungen des OAIS-Modells zentrale elektronische Archive sind, die meist durch staatliche Akteure oder Privatunternehmen betrieben werden. In diesem Zusammenhang ist auch davon auszugehen, dass diese dann auch die Rolle des Zertifizierungsdienstanbieters einnehmen oder einen externen Dienstleister damit beauftragen, ergo das System mit einem TTP-basierten Trusted-Timestamping-Dienst zu vergleichen wäre.

In Bezug auf die kryptografische Funktionsweise wird hierbei aber wie bei PoE ebenfalls auf als sicher geltende Hashing-Algorithmen zurückgegriffen (DIN 31647, 2015, S. 17–18). Die Norm legt jedoch zur Erzeugung, Prüfung, Nachsignierung und Hasherneuerung der Beweisdaten konkret RFC 4998 oder einen gleichwertigen Evidence Record Syntax-Standard fest. Ebenfalls erfordert sie, dass gesetzliche Vorgaben beim Signieren (SigG, SigV) eingehalten werden müssen. (DIN 31647, 2015, S. 17–20.)

Auch wenn DIN 31647 nicht die technische Umsetzung beschreibt, benennt sie akute praxisrelevante Aspekte, die PoE-Anbieter mangels fehlendem einheitlichen Standard oft unberücksichtigt lassen, etwa die Rechtsgültigkeit, das Verhältnis zu Aufbewahrungsfristen und die langfristige Erhaltung der kryptografisch angefertigten Nachweise.

Eine konkrete Beziehung zur Anwendung auf der Blockchain bzw. durch DLT stellt erst die Technische Spezifikation[20] DIN/TS 31648 von 2021 her. Sie legt „fachliche und technische Kriterien zur Anwendung der Blockchain und Distributed Ledger Technolo-

18 „Eignung eines Beweismittels, die Überzeugung eines Dritten, insbesondere eines Gerichts, zu beeinflussen“ (DIN 31647, 2015, S. 8).

19 „Methoden und Daten, die zur langfristigen Prüfung der Authentizität und Integrität elektronischer Dokumente notwendig sind“ (DIN 31647, 2015, S. 9).

gie (DLT) für vertrauenswürdige digitale Transaktionen sowie der notwendigen Berechtigungsmodelle aus Sicht der Nachweisfähigkeit (Records Management) und Beweiswerterhaltung fest“ (DIN/TS 31648, 2021, S. 6).

Als Anwendungsbeispiele werden u. a. genannt:

- *„Beweissichere Langzeitspeicherung aufbewahrungspflichtiger Unterlagen in regulierten Industrien/Branchen (Jahrzehntelange Fristen)*
- *Zugriff mehrerer Parteien auf einen definierten und vertrauenswürdigen Datenbestand*
- *Dokumenten/Datenverifikation“*

(DIN/TS 31648, 2021, S. 29.)

Die Technische Spezifikation ist vor allem vor dem Hintergrund entstanden, dass viele Branchen beim Einsatz von Blockchain bzw. DLT hinsichtlich eines ordnungsgemäßen Record Managements sowie der Beweiswerterhaltung den regulatorischen Vorgaben entsprechen müssen. Als Fundament herangezogen wird hierbei der Records Management Standard nach ISO 15489 und die EU-Verordnung Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG4 (eIDAS). (DIN/TS 31648, 2021, S. 5, 13, 15.)

Zum eIDAS-Verfahren ist hier angemerkt, dass die „Vertrauenswürdigkeit digitaler Transaktionen[21] [...] auf deren Prüfbarkeit durch vertrauenswürdige Dritte [beruht]“, die „durch die Verwendung vertrauenswürdiger digitaler Identitäten und Identifizierungsverfahren sowie (qualifizierter) elektronischer Signaturen, Siegel, Zeitstempel und Bewahrungsdienste nach eIDAS-Verordnung [erreicht wird]“ (DIN/TS 31648, 2021, S. 14).

Aufgrund seiner Technologieoffenheit kann die eIDAS zwar auf Blockchain bzw. DLT angewendet werden, nach der Bewertung der Spezifikation können diese aber die „signifikanten Eigenschaften geschäftsrelevanter Aufzeichnungen[22]“ alle nur bedingt erfüllen (DIN/TS 31648, 2021, S. 14–15).

In dem Zusammenhang verlangt die Spezifikation als weitere Kernanforderung (DIN/TS 31648, 2021, S. 15):

> *„[...] [D]ie* ***ausschließliche Nutzung einer*** **private permissioned** ***Blockchain/DLT****. Die* ***Inhalts- und Metadaten*** *geschäftsrelevanter Aufzeich-*

20 Hierzu sei eingangs der Hinweis aus dem Vorwort wiedergegeben: „Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, die wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird“ (DIN/TS 31648, 2021, S. 4).

21 Diese „ermöglichen den eindeutigen wie verlustfreien Nachweis der Authentizität, Integrität und Zuverlässigkeit der bei der Transaktionsabwicklung entstehenden oder empfangenden geschäftsrelevanten Aufzeichnungen bis zum Ablauf der geltenden Aufbewahrungsfristen gegenüber Gerichten, Prüfbehörden, Dritten“ (DIN/TS 31648, 2021, S. 13).

22 Authentizität, Integrität, Zuverlässigkeit, Vertraulichkeit, Verfügbarkeit und Verkehrsfähigkeit (DIN/TS 31648, 2021, S. 13).

> *nungen werden dabei* **off-chain**[23] *gespeichert. Nur die* ***Transaktionsdaten befinden sich*** **on-chain**[24]*."* [Hervorhebungen im Original.]

Um die Vorgaben an vertrauenswürdige Transaktionen des Weiteren erfüllen zu können, muss die Blockchain bzw. DLT laut der Spezifikation außerdem um Methoden des PoE und Rehashings[25] ergänzt werden.

PoE hat hier „aktuell durch den qualifizierten Zeitstempel eines qualifizierten Vertrauensdiensteanbieters" gemäß eIDAS zu erfolgen (DIN/TS 31648, 2021, S. 16). Konkret ist damit die Möglichkeit gemeint, „einzelne Transaktionen oder ganzen Blöcken der Blockchain bzw. DLT einen qualifizierten Zeitstempel nach ETSI EN 319422 sowie RFC 3161 hinzuzufügen" (DIN/TS 31648, 2021, S. 25).

Im Fall des Rehashings muss das RFC 4998 (Hashtree-renewal) oder ein gleichwertiger Evidence Record Syntax-Standard zum Einsatz kommen (DIN/TS 31648, 2021, S. 10, 24).

Neben den eben ausgeführten PoE-relevanten Aspekten trifft die Spezifikation darüber hinaus viele präzise fachliche und technische Kriterien zum Einsatz von Blockchain bzw. DLT im Records Management.

3.4 Ein Blockchain-basiertes Open-Science-Ökosystem

Nachdem im Verlauf der vorherigen Abschnitte die fundamentalen technischen Aspekte des PoE-Verfahrens herausgearbeitet wurden, legt dieser Abschnitt nun die Grundlagen eines Blockchain-basierten Open-Science-Ökosystems dar. Am Schluss dieser Darstellung werden entsprechende Kriterien zur Auswahl eines auf Open Science ausgerichteten PoE-Verfahrens formuliert, die dann in der darauf folgenden Evaluation zur Verwendung kommen.

Die für die Evaluation adaptierten Kriterien in dieser Arbeit stützen sich auf einen Kriterienkatalog von Leible et al. (2019), die in ihrer Studie die Charakteristika der Blockchain-Technologie mit den Zielen und Bedürfnissen der Open Science verglichen und daraus Anforderungen an ein Blockchain-basiertes Open-Science-Ökosystem erarbeitet haben (S. 3).

3.4.1 Definition von Open Science

Wie es die UNESCO (2021) zuletzt in ihrer Recommendation on Open Science niedergelegt hat, handelt es sich bei dieser offenen Wissenschaft um ein neues Paradigma:

---

23 „[M]it Bezug zu einer Blockchain/DLT, aber außerhalb der Blockchain befindlich oder ausgeführt. Beschreibt den eigentlichen Ort der Datenhaltung" (DIN/TS 31648, 2021, S. 9).

24 „[A]uf einer Blockchain/DLT befindlich oder ausgeführt. Beschreibt den eigentlichen Ort der Datenhaltung" (DIN/TS 31648, 2021, S. 9).

25 „[B]ezeichnet die Neuverhashung aller nicht mehr sicherheitsgeeigneten technischen Beweisdaten und sonstigen mit dem Hashbaum gesicherten Daten mit einem neuen sicherheitsgeeigneten Hashalgorithmus, bevor die Sicherheitseignung des bestehenden Hashalgorithmus abläuft" (DIN/TS 31648, 2021, S. 10).

> *„Building on the essential principles of academic freedom, research integrity and scientific excellence, open science sets a new paradigm that integrates into the scientific enterprise practices for reproducibility, transparency, sharing and collaboration resulting from the increased opening of scientific contents, tools and processes“* (S. 7).

Open Science wird hier definiert als:

> *„an inclusive construct that combines various movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community. It comprises all scientific disciplines and aspects of scholarly practices, including basic and applied sciences, natural and social sciences and the humanities, and it builds on the following key pillars: open scientific knowledge, open science infrastructures, science communication, open engagement of societal actors and open dialogue with other knowledge systems“* (S. 7).

Zusammengefasst lässt sich also festhalten, dass Open Science

- die wissenschaftliche Zusammenarbeit sowie das Teilen von Wissen zum Wohle von Wissenschaft und Gesellschaft fördert;
- wissenschaftliche Erkenntnisse über Sprachgrenzen hinweg global für jede*n verfügbar, zugänglich und wiederverwendbar macht;
- auch Personen außerhalb der Scientific Community den Zugang zum Wissenschaftsbetrieb ermöglicht.

(UNESCO, 2021, S. 8.)

3.4.2 Prinzipien einer auf Open Science ausgerichteten technischen Infrastruktur

Die oben herangezogene Recommendation der UNESCO nennt auch Open-Science-Infrastrukturen als einen zentralen Baustein von Open Science und fasst diese auch in eine Definition, die ziemlich universell ausfällt. Essenziell lässt sich dabei festhalten, dass hierunter Forschungsinfrastruktur verstanden wird, die der Unterstützung von Open Science dient und die Bedürfnisse der angeschlossenen Community(s) erfüllt. Als wichtigste Komponenten werden dabei Open-Science-Plattformen und Repositorien für Publikationen, Forschungsdaten und Quellcode als auch Software-Entwicklung und virtuelle Forschungsumgebungen oder digitale Forschungsdienste hervorgehoben. (UNESCO, 2021, S. 12.)

Nach Leible et al. (2019, S. 5) zählen zu den allgemeinen Anforderungen an eine auf Open Science ausgerichtete technische Infrastruktur:

- Eine kollaborative Umgebung
- Open Data
- Open Access
- Zensurfreiheit
- Identitäts- und Reputationsmanagement
- Erweiterbarkeit

Spezielle Anforderungen kommen aus den verschiedenen Open-Science-Denkrichtungen hinzu (Leible et al., 2019, S. 6–7):

- Demokratischer Ansatz: Anreize für die Partizipation am System, Gleichbehandlung aller Teilnehmenden
- Pragmatischer Ansatz: Einfache Integration in bestehende Workflows, Anreize für das Teilen von Daten und Inhalten
- Öffentlicher Ansatz: Möglichkeit für Crowdfunding, Offenlegung des Forschungsprozesses, Anbindung an Citizen Science
- Infrastruktureller Ansatz: Nutzung von Open Source und Open Sourcing von eigenem Code und eigenen Tools, gemeinsame Nutzung von Ressourcen
- Metrischer Ansatz: Metriken, Integration von internen und externen Systemen

3.4.3 Für Open Science relevante Charakteristika der Blockchain-Technologie

Als für Anwendungsfälle der Open Science relevante Charakteristika der Blockchain-Technologie haben Leible et al. (2019, S. 8–9) folgende herausgearbeitet:

- Dezentralisierung: Die Blockchain oder Teile davon werden redundant in einem verteilten P2P-System von Knoten gespeichert, deren Architektur es ermöglicht, selbst Software und andere Inhalte automatisch über das Netzwerk zu verteilen. Durch den Ausschluss eines Single Points of Failure wird auch eine Abhängigkeit von einer zentralen Autorität, der vertraut werden muss, hinfällig.
- Kryptografisches Hashing: Jeder Block ist mittels einem kryptografisch Hash jeweils mit dem vorangegangen Block verbunden, sodass eine chronologische Abfolge entsteht. Neben dem Konsensmechanismus ist durch das Hashing sichergestellt, dass die komplette Kette, inklusive des Inhalts, nicht verändert werden kann. Eine Änderung eines bestimmten Hash-Werts beträfe auch alle nachfolgenden Hash-Werte, wodurch die gesamte Kette ungültig werden würde.
- Timestamping: Jeder Datensatz (Erstellung des Blocks, Transaktion, Speicherung von Daten) in einer Blockchain wird chronologisch mit einem Zeitstempel versehen (Timestamping). Durch dieses Timestamping entsteht Rückverfolgbarkeit, Transparenz und die gesamte Transaktionshistorie wird für Nutzer*innen ersichtlich. Time-

stamping in Kombination mit kryptografischem Hashing können beispielsweise als Proof of Existence für eine Information zu einem bestimmten Zeitpunkt dienen.

- Unveränderbarkeit: Das kryptografische Hashing und der dezentrale Validierungsprozess (Konsensmechanismus) sorgen dafür, dass Daten, die einmal auf der Blockchain gespeichert sind, nicht mehr verändert oder gelöscht werden können. Spezifische Angriffe wie die 51%-Attacke bleiben dabei außen vor.
- Konsensmechanismus: Der Konsens definiert wie Nutzer*innen Transaktionen auf einer Blockchain untereinander validieren. Seit dem initial auf der Bitcoin-Blockchain eingesetzten Proof-of-Work-Mechanismus wurden viele neue Methoden und Kombinationen bestehender Konsensverfahren entwickelt und in neuen Blockchains implementiert.
- Zugänglichkeit und Governance-System: Jede Blockchain definiert sich durch ihren Zugang (öffentlich, konsortial oder privat) und ihr Governance-System (permissionless oder permissioned), woraus sich auch wiederum entscheidet, für welche Anwendungsfälle diese in Frage kommen.

Die Autoren merken an, dass diese Aspekte aber keine Alleinstellungsmerkmale der Blockchain-Technologie sind, also auch andere Lösungen existieren, die eine oder mehrere dieser Eigenschaften erfüllen (Leible et al., 2019, S. 9).

3.4.4 Kriterien für ein Blockchain-basiertes Open-Science-Ökosystem

Anhand der eben beschriebenen Charakteristika der Blockchain-Technologie erläutern Leible et al. (2019) nun in der Folge die Anknüpfungspunkte dieser an eine Open-Science-Infrastruktur und leiten Empfehlungen ab (S. 9-13):

1. Es muss sich um eine öffentliche Blockchain handeln, da diese allein im Sinne von Open Science allen Menschen den uneingeschränkten Zugang zu dem auf ihr abgelegten Wissen gewährt. Hierbei muss zwischen den Vorteilen und Nachteilen einer permissioned und einer permissonless Blockchain abgewägt werden.
2. Ein kollaboratives Umfeld sollte für alle Nutzenden geschaffen werden, indem dezentral etwa durch einen demokratischen Ansatz über den Fortbestand des Netzwerks abgestimmt werden kann. Auf technischer Ebene ist dies durch den Konsensmechanismus auf der Blockchain festgesetzt, der allein schon deswegen aufrechterhalten werden muss, um die fortwährende Integrität und Konsistenz der Blockchain zu gewährleisten.
3. Die Unveränderbarkeit einer Blockchain sollte als Garant für Forschungs- und Zensurfreiheit verstanden werden.
4. Die Blockchain kann als unabhängige Plattform für Open Data dienen, da sie nicht von Dritten abhängig ist und entsprechend Urheber*innen selbst entscheiden können, ob und unter welchen Bedingungen ihre Forschungsarbeit dort veröffentlicht wird. Forschende können eigenständig die Existenz, Autorenschaft und Herkunft ihrer Daten auf der Blockchain nachweisen.

5. Eine auf Open Science ausgerichtete Blockchain sollte ein Open-Access-Repositorium für Wissen repräsentieren, entsprechend auch auf Paywalls verzichten.
6. Das Netzwerk sollte als Anreiz ein der Wissenschaft und Forschung entsprechendes Identitäts- und Reputationssystem abbilden. Über die Blockchain eingereichte Daten sollten auf die Urheber*innen referenzieren und öffentlich aufgelistet werden, um die Qualität und den Einfluss der Blockchain-Veröffentlichungen bestimmen zu können; dazu sollte auch ein Bewertungssystem eingesetzt werden. Die Dezentralisierung und der Konsensmechanismus garantieren auf diese Weise ein organisches Entstehen von Reputation. Darüber hinaus könnten anonyme oder pseudonyme Einreichungen mittels Hashing möglich gemacht werden.
7. Genau wie andere IT-Infrastruktur muss die Blockchain erweiterbar sein, etwa durch Schnittstellen (APIs) zu anderen Systemen.
8. Anreize zur Teilhabe an der Blockchain müssen geschaffen werden. Dies kann durch verschiedene Möglichkeiten erreicht werden, etwa durch ein Angebot eines Proof-of-Existence-Dienstes als Garantie für Sicherheit, die Stimulation des Geben-und-Nehmen-Instinkts, oder auch die Ausgabe von Tokens an die Teilnehmenden als Wertanlage.
9. Auf der Basis von Dezentralisierung und dem entsprechenden Konsensmechanismus sollte auf dem Netzwerk ein gleichberechtigtes Beteiligungs- und Governance-Modell geschaffen werden, das von einer zentralen Autorität entkoppelt ist. Dadurch entsteht eine der Open Science entsprechende Infrastruktur, die allen Menschen den Zugang zur Wissenschaft eröffnet und die gleichen Chancen bietet, sich selbst Wissen anzueignen und sich weiterzubilden.
10. Die Integration der Blockchain in bestehende Systeme und Prozesse muss einfach und ohne ernsthaften Aufwand oder Kosten möglich sein. Dies kann durch eine angemessene Dokumentation, ein durchdachtes Netzwerkdesign und eine individuelle, leicht zu bedienende Schnittstelle (API) gelingen. Das bedeutet auch, bei der Wahl des Konsensmechanismuses zu berücksichtigen, wie viele Ressourcen (Speicherplatz, Rechenleistung) aufgebracht werden müssen, um am Netzwerk teilzunehmen.
11. Bevor Daten und Inhalte auf der Blockchain geteilt werden, sollten diese durch den Konsensmechanismus geprüft werden, etwa um Redundanz oder Schadsoftware zu vermeiden. Urheber*innen sollten die Möglichkeit haben, den Zugriff auf ihre Inhalte zu beschränken (Moratorium). Die Daten könnten entweder bis zur Freigabe verschlüsselt auf der Blockchain abgelegt werden oder auch off-chain, etwa in einer konventionellen Datenbank oder auf einem verteilten Dateisystem – in dem Fall wird nur eine Prüfsumme der Daten auf die Blockchain geschrieben.
12. Über den Konsens oder Smart Contracts könnten auf einer Blockchain auch Methoden zur Forschungsprojektfinanzierung umgesetzt werden, etwa durch ein Tokensystem oder die Anbindung an traditionelle Online-Bezahldienste. Durch das kryp-

tografische Hashing von Pseudonymen wären auch anonyme Beteiligungen möglich.

13. Die Reproduzierbarkeit von Wissenschaft und Anerkennung von Forschungsleistung könnte dadurch gestärkt werden, indem gesamte Verläufe von Forschungsprojekten auf der Blockchain nachgewiesen werden. Mittels Timestamping besteht die Möglichkeit, von der Idee über Studiendesign bis hin zum fertigen Paper alle Daten manipulationssicher als Hashes auf der Blockchain zu verewigen. So kann Forschung transparent nachvollzogen und rückwirkende Änderungen ausgeschlossen werden.
14. Auch wissenschaftliche Laien könnten über die Blockchain befähigt werden, gewonnene Daten (z. B. Messdaten) dezentral, manipulationssicher und zur öffentlichen Einsicht von Forschenden einzuspeisen. Dies würde Citizen-Science-Aktivitäten fördern.
15. Der Quellcode der Blockchain als auch der auf ihre basierten Tools sollten offen (Open Source) sein. Die Offenlegung von Code schafft nicht nur Transparenz und eine Nachvollziehbarkeit von den zugrundeliegenden Algorithmen, sondern ermöglicht auch die Weiterentwicklung durch die gesamte Community zugunsten des gesamten Ökosystems. Die Verschlüsselung von nicht für den offenen Zugang gedachten Tools und Code sollte aber gewährleistet sein. Die Dezentralisierung und Nachweisbarkeit von gesamten Forschungsverläufen auf der Blockchain kann beim Management und Nachvollziehen von Open-Source-Projekten hilfreich sein.
16. Die dezentrale P2P-Architektur der Blockchain könnte zum Verteilten Rechnen für Forschungszwecke genutzt werden. Eine faire Verteilung der zur Verfügung stehenden Ressourcen wäre über den Konsensmechanismus möglich. Forschende wären so etwa imstande, Experimente auf dem Netzwerk durchzuführen, die ihnen anderweitig mangels Ressourcen nicht möglich wären.
17. Die Blockchain könnte als vertrauenswürdige offene Plattform für das Erheben von Metriken genutzt werden. Durch die Dezentralisierung und den Konsensmechanismus wäre sie als Quelle für akkurate und verlässliche Metriken geeignet, da jeder Knoten im Blockchain-Netzwerk bei der Kalkulation und Verifizierung von Kennzahlen mitwirken kann.
18. Die Blockchain könnte mit internen und externen Systemen so integriert werden, dass diese untereinander Daten austauschen können. Mit bestimmten APIs wäre es sogar möglich, die Dateiverteilung über Systemgrenzen hinweg zu automatisieren, also etwa lokal abgelegte Forschungsdaten automatisch in eine angeschlossene Infrastruktur zu übertragen.
19. Für die langfristig Finanzierung einer auf Open Science ausgelegten Blockchain könnte ein Initial Coin Offering (ICO), die Ausgabe von Anteilen in der Form von Kryptowährung oder Token an Investoren, in Betracht gezogen werden. Jedoch sollte hierbei beachtet werden, dass damit Wissenschaft und Geschäftsinteressen unvermeidbar miteinander verschmelzen.

3.4.5 Kriterien zur Auswahl eines auf Open Science ausgerichteten PoE-Verfahrens

Aus den oben dargestellten Thesen von Leible et al. (2019) wurde für die vorliegende Arbeit ein Anforderungskatalog mit Ausrichtung auf Proof-of-Existence-Methoden erstellt. Anhand den unten aufgeführten Leitfragen soll im Folgekapitel die Evaluation ausgewählter PoE-Dienste durchgeführt werden.

Allgemeine Anforderungen

- Offener Zugang: Ist die Plattform für alle offen und gleich zugänglich? Kann die Plattform von allen genutzt werden? Gibt es etwa Einschränkungen durch Ressourcen, die für die Nutzung aufgebracht werden müssen?
- Zensurfreiheit: Ist die Plattform beeinfluss- oder zensierbar? Von wem wird die Plattform entwickelt und betrieben? Gibt es Regeln, wie entstehen diese bzw. wer stellt sie auf? (Governance)
- Identitäts- und Reputationsmanagement: Können Forschende sich auf der Plattform mit ihrer Identität ausweisen und ihre Leistungen referenzieren?
- Erweiterbarkeit: Ist die Plattform auf neue Entwicklungen anpassbar, erweiterbar und entsprechend nachhaltig strukturiert, dass Erweiterungen und Anpassungen auch für die Zukunft von der Community vorgenommen werden können?

Spezifische Anforderungen

- Demokratische Beteiligung: Können Änderungsvorschläge und Entscheidungen über den Fortgang der Plattform in einem demokratischen Prozess von allen Nutzenden gleichberechtigt eingebracht und getroffen werden?
- Anreize: Erhalten Forschende einen Gegenwert für ihre Beteiligung an dieser Community, etwa in Form von Coins, Tokens, Anerkennung oder Publicity?
- Workflow-Integration: Ist der Dienst der Plattform leicht in einen existierenden Forschungsworkflow einbindbar, etwa durch interoperable Schnittstellen (APIs)?
- Social-Sharing-Möglichkeiten: Ermöglicht die Plattform einen einfachen Weg, Daten und Inhalte zu teilen?
- Finanzierung: Kann die Finanzierung der Dienste von anderen oder kollektiv (etwa durch Crowdfunding) übernommen werden? Oder besteht auf irgendeine Art die Möglichkeit, einen Dritten zu honorieren, der im Auftrag für eine andere Person die Plattform nutzt?
- Transparenz und Nachvollziehbarkeit: Ist der Prozess, wer welchen Anteil bei der Erstellung des Datenobjekts beigetragen hat, mit dem Dienst abbildbar? Kann der Forschungsprozess mit allen Beteiligungen über den Dienst offen gelegt werden?
- Citizen Science: Ist der Dienst auch für den Daten-Output von Citizen-Science-Projekten geeignet?

- Open Source: Ist die Plattform Open Source, kann sie eventuell sogar auf eigenen Servern betrieben werden? Wurde der Dienst mit Open-Source-Software erstellt?
- Ressourcenschonung: Kann sich die Nutzung der Plattform zu Gunsten der Schonung von Ressourcen unter mehreren Teilnehmenden geteilt werden bzw. sind andere ressourcenschonende Verfahren aktiv?
- Metriken: Kann die Nutzung des Dienstes gemessen werden? Können Nutzende Statistiken zu ihren Daten einsehen?
- Kompatibilität: Ist der Dienst der Plattform mit eigener Software kombinierbar, etwa durch interoperable Schnittstellen (APIs)?

4 Evaluation

Zwei repräsentative Proof-of-Existence-Lösungen sollen nun in einer Evaluation anhand der im vorherigen Abschnitt entwickelten Kriterien eingeordnet und miteinander verglichen werden.

Zum einen ist es naheliegend, einen auf der Bitcoin-Blockchain basierenden PoE-Dienst zu untersuchen, da Bitcoin als dienstältestes Open-Source-Blockchain-Projekt mit einer der größten Entwickler*innen-Communitys und seiner weltweiten Verbreitung immer noch als das insgesamt beständigste Blockchain-Netzwerk überhaupt gelten kann. Als Forschungsgegenstand bietet sich hierfür OpenTimestamps an, das als Open-Source-Entwicklung inzwischen seit fast zehn Jahren besteht, dabei zugleich ein PoE-Verfahren, einen Dienst als auch einen Standard repräsentiert und bis heute Eingang in wissenschaftliche Arbeiten zu PoE findet, die es als eines der am meisten fortgeschrittenen Projekte beschreiben (Hyla & Pejaś, 2020, S. 2).

Zum anderen bietet es sich an, den bereits im Verlauf der Abhandlung erwähnten Zertifizierungsdienst der Wissenschafts-Blockchain Bloxberg als einen dezidiert auf Forschungsoutput ausgelegten PoE-Dienst näher zu betrachten. Hinter Bloxberg steht ein weltweites Konsortium reputabler Wissenschaftsorganisationen, darunter die Max-Planck-Gesellschaft, ETH Zürich, Georgia Institute of Technology, University of Johannesburg und weitere, wodurch es als bisher einzigartiges Blockchain-Projekt seiner Art gelten kann (Kleinfercher et al., 2020, S. 5–6). Im Bloxberg-Whitepaper, das durch alle Gründungsorganisationen gezeichnet wurde, finden sich einige Open-Science-Ansätze wieder, die das Projekt als besonders anschlussfähig für das in dieser Arbeit beschriebene Blockchain-basierte Open-Science-Ökosystem erscheinen lässt.

Um die technischen Abläufe bei den PoE-Diensten besser nachvollziehen zu können, wird hier im Rahmen der Evaluation die englischsprachige PDF-Veröffentlichung der UNESCO Recommendation on Open Science als Beispieldokument zur Erstellung eines Existenznachweises verwendet. Das Dokument (ark:/48223/pf0000379949) ist bei der UNESCO Digital Library abrufbar[26] und unter CC-BY-SA 3.0 IGO[27] lizenziert. Die Hashes der aktuellen Dokumentversion mit 36 Seiten, Erstellungsdatum Fr 03 Dez 2021 10:01:15 UTC, letztes Bearbeitungsdatum Sa 07 Mai 2022 14:37:34 UTC[28] sind die Folgenden:

- MD5: bbcd97299a3a61ab1c479e14b27069e2
- SHA1: 5594d25feb68ef457b090b44d7b66cdd218bbf14

26 https://unesdoc.unesco.org/ark:/48223/pf0000379949

27 http://creativecommons.org/licenses/by-sa/3.0/igo/

28 Die Datei ist alternativ archiviert über die Wayback Machine des Internet Archive zugänglich: https://web.archive.org/web/20220610131548/https://unesdoc.unesco.org/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_78a29cad-b57b-4f8f-803d-089a8313bf0f?_=379949eng.pdf&to=36&from=1

- SHA256: da3ba92c496d1b09b6342fad61b10f08cb309af82be6d47b3a59dabdcc60eaab

Die Hashes wurden auf Linux über die Kommandozeile mit den folgenden Befehlen erzeugt[29]:

```
$ md5sum 379949eng.pdf
$ sha1sum 379949eng.pdf
$ sha256sum 379949eng.pdf
```

Eine Entsprechung in Windows lässt sich dort über die PowerShell bewerkstelligen[30]:

```
Get-FileHash .\379949eng.pdf -Algorithm MD5
Get-FileHash .\379949eng.pdf -Algorithm SHA1
Get-FileHash .\379949eng.pdf -Algorithm SHA256
```

Deutlich nutzungsfreundlicher können aber auch Erweiterungen sein, die sich in den Datei-Manager bzw. Explorer integrieren und per Mausklick Hashes der ausgewählten Datei(en) erzeugen. Auf Windows eignen sich dafür z. B. Programme wie OpenHashTab[31] oder 7-Zip[32], die sich auch automatisch in das Explorer-Kontextmenü integrieren. In einigen Linux-Distributionen bzw. deren mitgelieferten Datei-Managern ist eine Prüfsummen-Funktion bereits standardmäßig integriert oder es wird auf das Programm GtkHash[33] zurückgegriffen.

Wie aber bereits in den Grundlagen zu PoE-Diensten erwähnt, wird das Erzeugen des Hashes den Nutzer*innen in der Regel von dem jeweiligen Anbieter über eine Web-Oberfläche, also im Browser, angeboten, ohne das externe Programme genutzt werden müssen. Aus Sicherheitsgründen oder im Fall von sehr großen Dateien[34] kann es jedoch empfehlenswert sein, diese separat selbst zu generieren und dann nur noch an den PoE-Dienst zu übergeben, insofern dieser die Möglichkeit dazu bietet.

Die Metadaten über die Erstellung und Änderung eines PDF-Dokuments lassen sich plattformübergreifend jedem gängigen PDF-Viewer mittels Aufrufen der Dokumenteigenschaften entnehmen.

4.1 Bitcoin-basierte PoE-Verfahren am Beispiel OpenTimestamps

OpenTimestamps besteht offiziell seit 2016, die Entwicklung wurde aber bereits 2012 durch den damaligen Bitcoin-Core-Mitentwickler Peter Todd begonnen und wird bis

29 https://wiki.ubuntuusers.de/Hashfunktionen/

30 https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash

31 https://github.com/namazso/OpenHashTab

32 https://www.7-zip.org

33 https://gtkhash.org

34 Die Dauer des Hashings einer Datei hängt immer von dem verwendeten Hash-Algorithmus und der Dateigröße in Kombination mit der dafür zur Verfügung stehenden Rechenleistung des Computers und der Leserate der Daten von dem Speichermedium ab.

heute überwiegend von diesem betreut (Todd, 2016). Das Projekt kann damit als eine der ältesten oder auch die älteste PoE-Implementierung der Welt bezeichnet werden[35].

Verschiedene große Blockchain Attestation Services wie z. B. Stampery oder Blocknotary, die für sich wiederum unterschiedliche Branchen bedienen, greifen auf OpenTimestamps zurück, indem sie dessen Codebasis für den Betrieb ihrer eigenen PoE-Dienste verwenden. Kleinere Firmen nutzen hingegen vielmehr die durch OpenTimestamps bereitgestellten öffentlichen Server, um sich Existenznachweise für ihre jeweiligen Use Cases zu erstellen. (GitHub, 2022c; OpenTimestamps.Org, 2022, Abschn. „Members“.)

4.1.1 Technische Eigenschaften

Die technische Umsetzung von OpenTimestamps basiert auf einem Client-Server-Prinzip (siehe dazu den vollständig dokumentierten PoE-Ablauf in Anhang A, im weiteren Verlauf werden nur relevante Ausschnitte verwendet).

Über die OpenTimestamps-Client-Implementierung[36] ist das Erstellen der Existenznachweise als auch deren Verifizierung möglich (Todd, 2016, Abschn. „Creating and Validating Timestamps“). Der Client wird üblicherweise lokal installiert und über die Kommandozeile bedient. Auf der offiziellen Website opentimestamps.org ist jedoch auch eine rein über den Browser nutzbare Variante zu finden (siehe Abbildung 6). Implementierungen von OpenTimestamps sind darüber hinaus derzeit in Python[37], Javascript[38] und Java[39] verfügbar. Weitere Umsetzungen gibt es zwar auch in Rust[40] und Haskell[41], diese wurden aber schon länger nicht mehr aktualisiert.

Der Server[42], auch Calendar-Server genannt, fungiert letztendlich als eine Art Cache für anstehende PoE-Nachweise auf einer permissionless Blockchain, um die Ausstellung der Existenznachweise an die Nutzer*innen zu beschleunigen, die sich normalerweise aufgrund der langen Wartezeit bis zur Verankerung der Transaktionen in die Blockchain deutlich verzögern würde. Er nimmt zuerst die zuvor durch die Clients erstellten und verfremdeten Dokumentenhashes entgegen, aggregiert all diese in kurzen Zeitabständen in einem Merkle Tree und bewahrt davon nur den Merkle Root (Top Hash) auf. Beim Hashing wird dabei durchgehend das SHA256-Verfahren genutzt. Der jeweilige anfragende Client erhält vom Calendar-Server sofort jeweils eine vorläufige .ots Attestierungsdatei (OpenTimestamps Proof) ausgegeben, die den se-

35 Dies lässt sich auch anhand der Erstellungsdaten der GitHub-Repositorien und der enthaltenen Commits belegen. Etwa wurde das Repository opentimestamps-server am 05.10.2012 auf GitHub erstellt (GitHub, 2022f, Key-Eintrag „created_at“). Der erste Commit erfolgte bereits am 09.06.2012 (GitHub, 2022e).

36 https://github.com/opentimestamps/opentimestamps-client

37 https://github.com/opentimestamps/python-opentimestamps

38 https://github.com/opentimestamps/javascript-opentimestamps

39 https://github.com/opentimestamps/java-opentimestamps

40 https://github.com/opentimestamps/rust-opentimestamps

41 https://github.com/opentimestamps/experimental-haskell-opentimestamps

42 https://github.com/opentimestamps/opentimestamps-server

quenziellen Ablauf des Hashings seines jeweiligen Dokumentenhashs bis hinauf zu dem Merkle Root auf dem Server enthält. In einem Folgedurchlauf erstellt der Calendar-Server aus den sich angesammelten Top Hashes der verschiedenen Merkle Trees mit PoE-Anfragen wiederum einen Merkle Tree dessen Merkle Root schließlich in die Bitcoin-Blockchain geschrieben wird. Über die Browservariante oder den Client können sich die Nutzer*innen dann nach der erfolgten Verzeichnung in der Blockchain die endgültige Attestierungsdatei herunterladen, die den kompletten sequenziellen Ablauf ab dem Hashings des Dokuments bis hin zum Block-Header auf der Blockchain beinhaltet. (Todd, 2016, Abschn. „How OpenTimestamps Works“.)

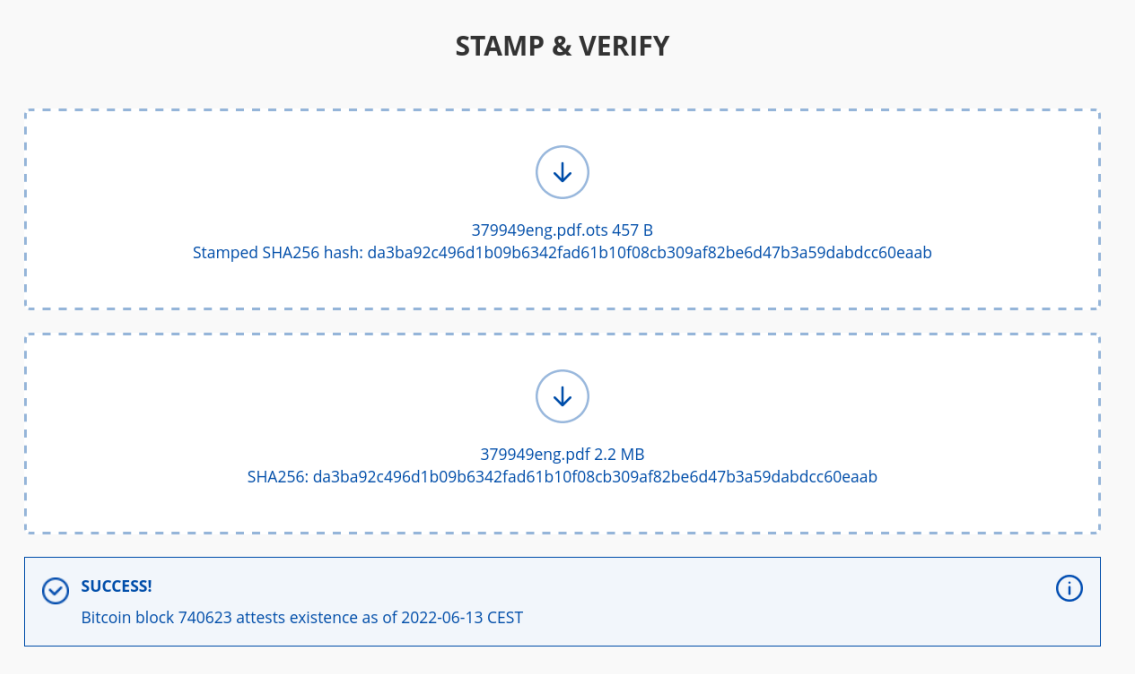
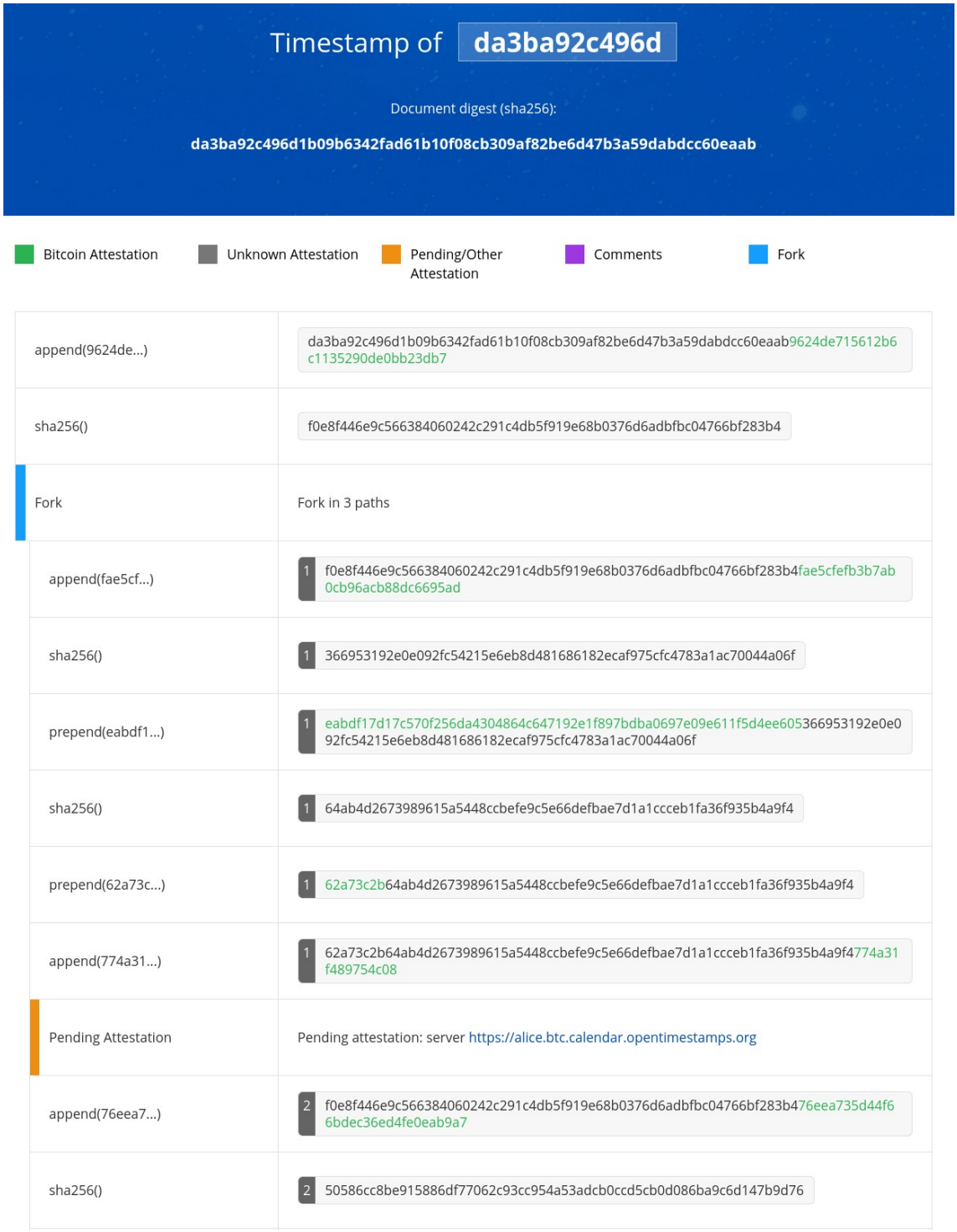


Abbildung 6: Existenznachweis mittels der Browservariante von OpenTimestamps

Das Format der .ots Attestierungsdatei ist Blockchain-agnostisch gehalten, es könnte also theoretisch ein Calendar-Server für eine andere Blockchain angebunden werden, der dann die in der Datei enthaltenen Sequenz der Hashes vom Dokument bis zu dem Block-Header auf dieser jeweiligen Blockchain zurückführen kann. Diese Eigenschaft macht deutlich, dass hiermit ein Standard für ein PoE-Verfahren angestrebt wird. De facto wird aber aktuell aufgrund mangelnder Nachfrage der Umsetzung auf anderen Blockchains die Weiterentwicklung abseits von Bitcoin vernachlässigt (Todd, 2019).

Die .ots Attestierungsdateien sind Binärdateien, sie können also nicht im Klartext angesehen werden. Nach Angaben des OpenTimestamps-Gründers ist dies bewusst so gehalten, um Fehler bei der Interpretation und Deutung durch verschieden implementierte Interpreter zu vermeiden. Gegen die Formate JSON oder XML habe er sich im Laufe der Entwicklung entschieden, weil diese bei der Interpretation eine gewisse Fehlertoleranz zuließen, die aber bei Attestierungsdateien aus Sicherheitsgründen absolut vermieden werden müsste. (Weilbach, 2017, S. 55–57.) Der OpenTimestamps-Client als

auch die Browser-basierte Variante verfügen jedoch über die Möglichkeit, die in der Attestierungsdatei enthaltenen Hashing-Sequenzen visuell darzustellen. Abbildung 7 zeigt die visuelle Darstellung der Sequenzen am Beispiel der vorläufigen Attestierungsdatei des Beispieldokuments 379949eng.pdf, wenn diese über die OpenTimestamps-Website aufgerufen wird[43].



43 Die visuelle Abbildung der sequenziellen Abläufe einer endgültigen Attestierungsdatei ist sehr umfangreich, deswegen wurde aus Platzgründen davon abgesehen, eine solche in diesem Dokument einzufügen.

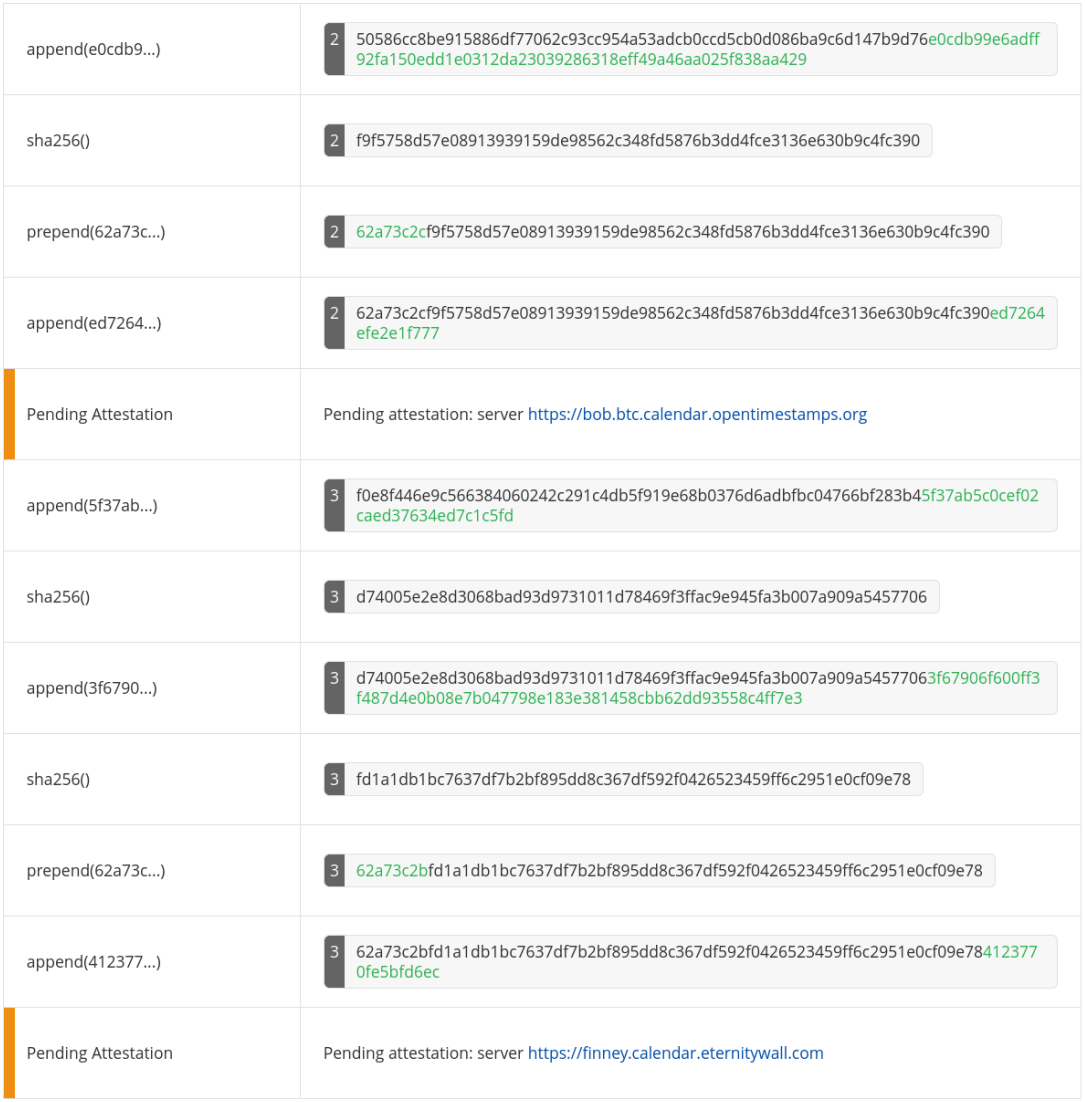


Abbildung 7: Visuelle Darstellung der Hashing-Sequenzen von OpenTimestamps

Hier ist zu sehen, dass die Attestation an drei der öffentlichen Calendar-Server gleichzeitig weitergegeben wurde, hier als Fork bezeichnet, und die Attestierung auf der Blockchain noch durch alle Server bevorsteht (Pending Attestation). Die in den Zeilen vorangestellte Zahl (1, 2 oder 3) sind ein visuelles Hilfsmittel zur Unterscheidung zwischen auf den jeweiligen Servern durchgeführten Hashingabläufen. Im Fall des Beispieldokuments wurde die Attestation letztendlich über Bob (Calendar-Server 2) am schnellsten verarbeitet (siehe Abbildung 6) und hat nach ungefähr 1 Stunde und 34 Minuten als erstes den Eingang in die Bitcoin-Blockchain erlangt. Somit ist der früheste Existenznachweis für die 379949eng.pdf auf der Bitcoin-Blockchain am 13.06.2022 um 15:05:47 UTC mit der Transaktion 474356a004a7e17bed81d87ff6867e5a78c07-ba8b378287f7bab2c21c0d3a259[44] im Block 740623[45] erfolgt. Die Attestierung durch Alice (Calendar-Server 1) folgte mit der Transaktion 73ecec9f5dcae-

44 https://blockstream.info/nojs/tx/474356a004a7e17bed81d87ff6867e5a78c07ba8b378287f7-bab2c21c0d3a259

45 https://blockstream.info/nojs/block/000000000000000000000206b4-ba8c9b158723e4a292830ad3a1f962988579178

b48d517a065697b4e5e5430953d4c9ae0ae540971f7aa3a6030[46] im Block 740642[47] und Finney (Calendar-Server 3) mit der Transaktion d82b0bcdd334e3edcbc44bf7a1f5e9edffec189a1846b9159327d529c64444ed[48] im Block 740683[49].

Die gesamte Ausgestaltung dieser Art von Implementierung ist darauf zurückzuführen, dass dieser PoE-Dienst in seinem Ursprung und seiner Ausrichtung nach wie vor auf der Bitcoin-Blockchain basiert. Die Transaktionskosten sind hier ein wesentlicher Einflussfaktor. Bei den großen öffentlichen Blockchains wie Bitcoin steigen die Transaktionskosten je nach Netzwerkauslastung[50]. Auf permissionless Blockchains basierende PoE-Dienste wie OpenTimestamps setzen daher zum einem bewusst geringe Gebühren für ihre Transaktionen (low fee Transaktionen), um ihre finanziellen Ausgaben wirtschaftlich halten zu können. Der abschließende Prozess des Inkorporierens in die Blockchain kann aufgrund dieser niedrig gesetzten Transaktionsgebühren dann jedoch mehrere Stunden dauern[51]. Zum anderen greifen sie auf verschiedene Methoden in der Programmierung ihrer Dienste zurück, um möglichst viele Existenznachweise möglichst kompakt in einer Transaktion unterzubringen. Durch OpenTimestamps wurden so etwa 2017 mittels der Merkle-Tree-Methode die Existenznachweise von rund 750.000.000 Dateien des Internet Archives in einer einzigen Bitcoin-Transaktion untergebracht (Todd, 2017a). Für die besonders effiziente Verarbeitung vieler Anfragen an einen Calendar-Server wurde 2019 als Erweiterung ein High-Performance-Aggregator[52] entwickelt.

4.1.2 Anschlussfähigkeit an ein Blockchain-basiertes Open-Science-Ökosystem

OpenTimestamps spiegelt in vielen Aspekten der Gestaltung seiner Infrastruktur die selben Eigenschaften wider, die schon das Bitcoin-Blockchain-Projekt seit seiner Gründung ausmachen und sich auch heute zum Teil in den auf Open Science ausgerichteten Infrastrukturen wiederfinden.

Der Zugang steht jedem unter gleichen Bedingungen frei, sämtliche OpenTimestamps-Komponenten, selbst die Website, sind Open Source auf GitHub verfügbar[53]. Entsprechend könnten die einzelnen Teile des PoE-Dienstes auch durch interessierte For-

46 https://blockstream.info/nojs/tx/73ecec9f5dcae-b48d517a065697b4e5e5430953d4c9ae0ae540971f7aa3a6030

47 https://blockstream.info/nojs/block/000000000000000000040cabfe7c9f69e-f842116d3d7b82029ccf6a46d870ed1

48 https://blockstream.info/nojs/tx/d82b0bcdd334e3edcbc44bf7a1f5e9edf-fec189a1846b9159327d529c64444ed

49 https://blockstream.info/nojs/block/000000000000000000007082db580e0afa728c5e6c6872f94c83ffef62ef82009

50 Im Fall von Bitcoin betrug die Gebühr für eine Transaktion zu Spitzenzeiten bereits umgerechnet rund 60 US-Dollar (BitInfoCharts, 2022a).

51 Normalerweise dauert die Verarbeitung einer Transaktion auf der Bitcoin-Blockchain aktuell bei Entrichtung durchschnittlich hoher Transaktionsgebühren rund 10 Minuten, bis die Miner sie in den nächsten Block aufgenommen haben (BitInfoCharts, 2022b).

52 https://github.com/opentimestamps/foxglove

53 https://github.com/opentimestamps

schende oder Forschungsorganisationen auf der eigenen Hardware in Betrieb genommen, angepasst oder Coderevisionen eingereicht werden.

Deutlich hervorzuheben ist aber der Umstand, dass aktuell im Eigenbetrieb sowohl eines Calendar-Servers, aber auch für die Verifizierung einer Attestierung über die Client-Komponente die Anbindung an einen mit der Bitcoin-Blockchain synchronisierten Bitcoin-Knoten (Full Node) erforderlich ist. Das Aufsetzen eines Bitcoin-Knotens setzt voraus, dass in jedem Fall mindestens einmal die komplette Bitcoin-Blockchain in ihrer aktuellen Größe von über 400 GB (BitInfoCharts, 2022c) heruntergeladen werden muss. Im Fall des Clients gibt es aktuell Überlegungen zu einem ressourcenschonenden Verifizierungsmodus, der im Zusammenhang mit der Einbindung eines öffentlichen Block-Explorers[54] funktionieren soll (GitHub, 2022a).

Während auf der Bitcoin-Blockchain das Tätigen von Transaktionen die Bezahlung von Gebühren in Form von Bitcoins erfordert, stellt das OpenTimestamps-Entwicklerteam seit der offiziellen Inbetriebnahme von OpenTimestamps öffentliche Calendar-Server zur Verfügung, die durch sie selbst und Spenden auf die mit den Servern verbundenen Bitcoin-Wallets finanziert werden (OpenTimestamps.Org, 2022, Abschn. „Calendars“). Zu Anfang waren es drei öffentlich nutzbare Calendar-Server, im Jahr 2018 kam ein vierter hinzu (Todd, 2018b). Der aktuelle Spendenstand samt der Bitcoin-Wallet-Adresse ist immer auf der Website des jeweiligen Calendar-Servers einsehbar (siehe am Beispiel des öffentlichen Calendar-Servers Bob in Abbildung 8). Die Nutzung von OpenTimestamps ist also über die öffentlichen Server komplett kostenlos. Insofern der Betrieb durch Forschende oder deren Organisation auf eigenen Servern bevorzugt wird, müssten jedoch auch sämtliche entstehende Kosten (Servermiete, Blockchain-Transaktionsgebühren, Personalkosten für die Serverwartung etc.) selbst übernommen werden.

Eine Abhängigkeit von den durch das Entwicklerteam betriebenen öffentlichen Servern ist also bei Eigenbetrieb eines Calendar-Servers nicht gegeben. Der Attestierungsprozess von OpenTimestamps ist darüber hinaus allgemein mit Bedacht auf die Erhaltung der Privatsphäre gestaltet (siehe unten), sodass selbst bei Nutzung der öffentlich bereitgestellten Calendar-Server als Konsequenz höchstens zu befürchten wäre, dass eine Attestierungsanfrage nicht verarbeitet wird.

Im Web-Frontend eines Calendar-Servers[55] werden neben dem Spendenstand auch Statistiken über das aktuelle Nutzungsaufkommen und die letzten Attestations in HTML (siehe Abbildung 8) oder auch im JSON-Format ausgegeben. Retrospektive Metriken über Monate oder Jahre sind aktuell nicht implementiert. Bei Betrieb eines eigenen Ca-

54 Block-Explorer sind Web-Frontends, die Prozesse auf der Blockchain in Echtzeit im Browser abbilden und ebenso eine Such-Oberfläche für die auf der Blockchain enthaltenen Daten bereitstellen. Im Backend läuft dabei ein an die Blockchain angebundener Knoten. Gerade bei verbreiteten Blockchains wie Bitcoin oder Ethereum werden von verschiedenen Teilen der Community eigene Instanzen an Block-Explorern betrieben. Der Rückgriff auf Block-Explorer ist eine Frage des Vertrauens. Interaktionen mit der Blockchain sind auch unabhängig vom Web über einen eigenen Knoten möglich.

55 https://github.com/opentimestamps/opentimestamps-server/blob/master/otsserver/rpc.py

lendar-Servers ließen sich durch etwaige Anpassungen im Code die Nutzungsstatistiken sicherlich auch auf Dauer speichern und auswerten. Hierfür kann jedoch nicht wie etwa von vielen Open-Source-Forschungsrepositorien gewohnt direkt mit einer interoperablen API gearbeitet, sondern es muss sich zuerst mit der Bitcoin-eigenen RPC API[56] auseinandergesetzt werden, um ein Verständnis für die Blockchain-spezifischen Befehlsabläufe zu erlangen. Für die Kommunikation mit dem Bitcoin-Knoten an sich stehen dann auch gängige Interfaces wie JSON[57] oder REST[58] zur Verfügung.


This is an OpenTimestamps Calendar Server (v0.5.0)

Pending commitments: 10159
Transactions waiting for confirmation: 0
Most recent unconfirmed timestamp tx: None (0 prior versions)
Most recent merkle tree tip: None
Best-block: 00000000000000000023f2f304c864a83fc50906d2e3b945b4e8813edbebdc3, height 740791

Wallet balance: 0.00243063 BTC

You can donate to the wallet by sending funds to:

bc1qw64evsq4m6j7jlfpcannpj9yu0dp4f3ve38336

Average time between transactions in the last week: 8.84 hours
Fees used in the last week: 0.00012114 BTC

Latest mined transactions (confirmations):

a51745ab50f3bcdb9a4c138e625ef207fe4729d475be477dd9702bad17797bdc (42)
cb30e6710b021cb07abdc8a39377c8804e0899f8d9e044d967913e1a512e089c (111)
474356a004a7e17bed81d87ff6867e5a78c07ba8b378287f7bab2c21c0d3a259 (169)
b409339836d97aba1fa50a637900c09460aff280a5a6dd9a8ea6caa48ba9bdeb (224)
39bd456c0471bbee5fa0d357c4c11d672b35b10ec6aa96a1e38c7a20869f67c3 (266)
4f5220c49e02e5998b84d9e4693a15b9a0309170e0f0173a6f39a6820888c300 (301)
a2959fb0fa8c08634a7445173a3c79da1680150c877a26b01dacf57d0dad290e (351)
aa9c4aba62a823e93fdf0ffec0ba97b8a395dee0e19fd0d4036144b90d9bc1cd (415)
5f16e84d914d38c130ccc0ba7ca4593b25cb310e370fd80e266e7a3b5064289a (484)
e32f98c93a07d86e46a73f3c547a6e87b8b63b42559e4e8e7bf2886f09ed705f (529)

Abbildung 8: Web-Oberfläche eines OpenTimestamps Calendar-Servers

Aufgrund dessen, dass OpenTimestamps aktuell ausschließlich auf Basis der Bitcoin-Blockchain betrieben wird, greifen hinsichtlich Zensurfreiheit und Governance grundsätzlich einmal die Gegebenheiten auf der Bitcoin-Blockchain. Wie bereits im Grundlagen-Kapitel dargelegt, ist das Bitcoin-Netzwerk wegen seiner Beständigkeit und der großen Entwickler*innen-Community als eines der resilientesten Blockchain-Netzwerke der Welt einzustufen.

56 https://developer.bitcoin.org/reference/rpc/
57 https://github.com/bitcoin/bitcoin/blob/master/doc/JSON-RPC-interface.md
58 https://github.com/bitcoin/bitcoin/blob/master/doc/REST-interface.md

Die Entscheidungsfindung innerhalb der Bitcoin-Community ist so vielschichtig, wie die verschiedenen Interessengruppen, die sich bei Entscheidungen gegenüber stehen. Neben einem festen Kreis von Bitcoin-Entwickler*innen[59], gibt es viele weitere nur vorübergehende Beteiligte[60], Miner-Zusammenschlüsse (Mining-Pools)[61] und natürlich investierte Unternehmer*innen und Privatpersonen. Personen, denen besonderer Einfluss zugerechnet wird[62], verfügen jedoch nicht über besondere Stimmrechte. Die Gründungsfigur Satoshi Nakamoto hat 2011 die leitende Position in der Entwicklung von Bitcoin abgegeben und seine Beteiligung eingestellt (Rizzo, 2021). Die Entwicklung des Bitcoin-Codes erfolgt seit der Erstveröffentlichung durch Nakamoto auf GitHub[63].

Ähnlich wie die Scientific Community findet die Bitcoin-Community sich zum Austausch regelmäßig auf Meetups[64], Konferenzen[65] und anderen Veranstaltungen zusammen. Die aktivsten Kommunikationskanäle sind jedoch Mailinglisten, Online-Foren und Chats. Online ist die Community oft noch mal in verschiedene Unter-Communitys aufgespalten, die sich ausschließlich mit bestimmten Themengebieten wie z. B. Entwicklung, Mining oder Investment beschäftigen. Eine Beteiligung steht jedem auf allen Plattformen offen und ist freiwillig.

Änderungsvorschläge müssen aber letztendlich immer in ein Bitcoin Improvement Proposal (BIP) münden, das dann durch jede*n im Bitcoin-Repository auf GitHub öffentlich eingesehen werden kann[66]. Die genaue Verfahrensweise und alle Prozesse dahinter sind aktuell durch das BIP 2[67] definiert. Die Debatten hinter einem solchen Prozess sind jedoch oft langwierig, eine schnelle Implementierung neuer Features ist daher selten[68]. Bis zur Umsetzung eines beschlossenen BIPs kann es teils Jahre dauern, weil letztendlich auch die Miner das mit der Entscheidung zusammenhängende Softwareupdate annehmen müssen. So gesehen definiert sich das Bitcoin-Protokoll de facto durch das Verhalten der am Bitcoin-Netzwerk beteiligten Validatorknoten und nicht allein durch schriftlich festgehaltene Statements. Die Machtverteilung bei den Minern kann als problematisch angesehen werden, weil bestimmte Mining-Pools immer wieder zeitweise zusammen über die Hälfte der Mining-Rechenleistung des Bitcoin-Netzwerks repräsentieren[69]. Die 51% sind bei einem Blockchain-Netzwerk mit PoW-Konsensmechanismus die kritische Schwelle, die überwunden werden muss, damit Angreifende

59 https://github.com/bitcoin/bitcoin/blob/master/contrib/builder-keys/keys.txt

60 https://bitcoin.org/en/development#bitcoin-core-contributors

61 https://www.blockchain.com/pools

62 https://en.bitcoin.it/wiki/People

63 https://github.com/bitcoin/bitcoin

64 https://en.bitcoin.it/wiki/Meetups

65 https://en.bitcoin.it/wiki/Conferences

66 https://github.com/bitcoin/bips

67 https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki

68 Ein populäres Beispiel dafür ist das sogenannte New York Agreement, ein im Mai 2017 geschlossener Kompromiss, der eine jahrelang andauernde Debatte um die maximale Größe eines Bitcoin-Blocks beendete (Bitcoin Wiki, 2018b).

69 https://www.blockchain.com/charts/pools-timeseries

Manipulationen an den Transaktionen vornehmen können, auch 51%-Attacke genannt (Bitcoin Wiki, 2020, Abschn. „Attacker has a lot of computing power“). In dem Zusammenhang wurde bereits 2012 durch die Bitcoin-Community festgehalten, dass hier das Prinzip der Economic Majority greift. Sollten Miner ohne Einverständnis der gesamten Community Änderungen durchsetzen, würde die restliche Community die ab diesem Punkt erzeugten Bitcoins nicht mehr im Tausch gegen andere Werteinheiten, Tauschmittel oder Dienstleistungen anerkennen und der damit einhergehende Wertverlust dieser Bitcoins würde somit letztendlich den Minern selbst schaden (Bitcoin Wiki, 2018a).

Zu OpenTimestamps muss angemerkt werden, dass hier der Entwickler*innenkreis deutlich kleiner ist[70] und mit Ausnahme von Peter Todd, der zeitweilig im Rahmen eines Kundenauftrags bezahlt an dem Projekt arbeiten konnte (Todd, 2016), niemand beständig und dezidiert für die Arbeit an dem Projekt angestellt ist. Einbringen können sich Interessierte hier auch über das GitHub-Repository oder eine Mailingliste[71]. Mit dem Open-Source-Gedanken als gängige Praxis bei der Entwicklung von sowohl den Softwarekomponenten der Bitcoin-Blockchain als auch des darauf basierenden OpenTimestamps sind aber grundsätzlich alle Möglichkeiten der Erweiterbarkeit, auch der anderweitigen Weiterführung der Entwicklung (Fork) etwa durch Entwickler*innen aus dem Open-Science-Ökosystem gegeben.

Das Bitcoin-Netzwerk selbst und auch OpenTimestamps ist auf Anonymität und die Wahrung der Privatsphäre ausgelegt, entsprechend finden sich dort auch bewusst keine Möglichkeiten für ein Identitäts- und Reputationsmanagement, wie es aus dem Umfeld von Forschungsrepositorien bekannt ist. OpenTimestamps bringt diese Prinzipien auch in seiner Implementierung zum Ausdruck:

- Bei der Erstellung der Attestierungssequenz wird dem Dokumentenhash vor der Übertragung an den Calendar-Server eine Nonce hinzugefügt, um den Ursprungshash des Dokuments zu verschleiern (Weilbach, 2017, S. 68–69)
- Es werden an keiner Stelle des PoE-Prozesses personenbezogene Daten abgefragt bzw. erhoben[72] und die Rückverfolgung anhand Transaktionsdaten oder Bezahlungsdienstleistern (etwa für den Umtausch von Euro in Bitcoins, um Transaktionsgebühren bezahlen zu können) entfällt, insofern auf die kostenlos nutzbaren öffentlichen Calendar-Server zurückgegriffen wird

Entsprechend kann bei OpenTimestamps der gesetzte Anreiz sein, dass sich hiermit möglichst anonym kostenlos Existenznachweise auf der am meisten etablierten Block-

70 Im OpenTimestamps-Repository auf GitHub sind öffentlich vier Mitglieder gelistet (GitHub, 2022d).

71 https://lists.opentimestamps.org/mailman/listinfo

72 Bezüglich der DSGVO-Konformität der Calendar-Server betont Todd (2018a), dass wie bei jeder Server-Applikation, die Zugriffe von außen erhält, als einzige Ausnahme die anfallenden Logdateien IP-Adressen enthalten können. Hier sollte in Betracht gezogen werden, diese zu anonymisieren und bzw. oder die Logs regelmäßig zu löschen. Laut seiner Aussage werden die durch das OpenTimestamps-Entwicklerteam gestellten öffentlichen Calendar-Server alle DSGVO-konform betrieben.

chain der Welt verewigen lassen können. Auf Social-Sharing-Möglichkeiten wird in der Hinsicht ebenfalls verzichtet.

Die Einbindung von OpenTimestamps in einen Forschungsworkflow ist grundsätzlich vorstellbar. OpenTimestamps unterstützt standardmäßig die Integration mit Git[73], sodass auch in Git-basierte Versionierungssysteme eingebundene Dokumente verarbeitet werden können. Jedoch steht für eine Integration in vorhandene Forschungssoftware keine interoperable API zu Verfügung, sodass der Ausgangspunkt einer Implementierung zwingend Python, JavaScript oder Java sein muss. Unabhängig davon bleibt Forschenden natürlich immer noch die Option, die Erstellung von Existenznachweisen manuell über den Browser durchzuführen.

Wie OpenTimestamps am Beispiel der Verarbeitung von Millionen von Dateien des Internet Archives bereits gezeigt hat, ist der Dienst in der Verarbeitung von Anfragen enorm skalierbar. Es können sich also auch etwa Citizen-Science-Projekte, die oftmals mit einem großem Daten-Output oder vielen Datasets arbeiten, effizient Existenznachweise über ihre Daten erzeugen. An dieser Stelle sei noch einmal darauf hingewiesen, dass PoE-Dienste wie OpenTimestamps explizit nicht für die Dateihaltung konzipiert sind, sondern nur die Hashes der Dateien verarbeiten. Im Umfeld der Wissenschaft kann davon ausgegangen werden, dass die Forschenden an ihren Forschungseinrichtungen für die Dateiablage bereits jeweils ihre individuellen Workflows etabliert haben.

4.2 Ethereum-basierte PoE-Verfahren am Beispiel Bloxberg

Das Bloxberg-Projekt wurde 2019 auf Initiative von Mitarbeiter*innen der Max Planck Digital Library (MPDL) gegründet. Die Bloxberg-Blockchain wurde am 10.01.2019 in Betrieb genommen (Bloxberg Mainnet Explorer, 2019). Im Februar 2019 wurde auf dem ersten Bloxberg Summit durch Repräsentant*innen von elf Wissenschaftsorganisationen aus neun Ländern der Konsensmechanismus und das Governance-Modell ausgehandelt und in einem Manifest zusammen niedergelegt, dass der Betrieb der Blockchain fortan konsortial erfolgen soll.

Zu den Gründungsorganisationen des Konsortiums zählen (Kleinfercher et al., 2020, S. 7):

- Max-Planck-Gesellschaft (Deutschland)
- Universität Nikosia (Griechenland)
- University College London (UK)
- IT-Universität Kopenhagen (Dänemark)
- Universität Kassel (Deutschland)
- Georgia Institute of Technology (USA)

73 https://github.com/opentimestamps/opentimestamps-client/blob/master/doc/git-integration.md

- Carnegie Mellon University (USA)
- Universität Johannesburg (Südafrika)
- Universität Sarajevo (Bosnien und Herzegowina)
- ETH-Bibliothek an der ETH Zürich (Schweiz)
- Universität Belgrad (Serbien)

Das Bloxberg-Konsortium hat inzwischen 34 Mitglieder (Bloxberg.Org, 2022, Abschn. „bloxberg Members“). Laut der Validators dApp existieren 38 Validatorknoten, darunter finden sich jedoch sieben leere Einträge (Bloxberg Validators DApp, 2022).

4.2.1 Technische Eigenschaften

Bloxberg ist eine permissioned Blockchain auf Ethereum-Codebasis mit PoA als Konsensmechanismus.

Als Gründe für die Entscheidung für ein solches System werden die Feststellungen genannt, dass:

- Ethereum eine der größten Entwickler*innen-Communitys hat und sich im Produktionsbetrieb als resilient, stabil und skalierbar erwiesen hat
- der PoA-Konsensmechanismus in Verbindung mit Ethereum die beste Kombination aus Sicherheit, Effizienz und Dezentralisierung bietet

(Kleinfercher et al., 2020, S. 10.)

Im Fall von PoW-basierten Blockchains wie Bitcoin können beliebige Akteure Rechenleistung durch das Mining einbringen und bleiben dabei prinzipiell anonym. Auf der Bloxberg-Blockchain gibt es kein Mining, sondern die hinzukommenden Blöcke werden von den Validatorknoten gemintet und die am Minting eines Blocks beteiligte Wissenschaftsorganisation ist immer offen sichtbar. (Kleinfercher et al., 2020, S. 12–13.)

Aufgrund des PoA-Konsensmechanismuses können Transaktionen viel schneller verarbeitet werden. Die Bestätigung einer Transaktion benötigt auf der Bloxberg-Blockchain momentan durchschnittlich 7 Sekunden (Bloxberg Mainnet Explorer, 2022), auf der Bitcoin-Blockchain dauert dies rund 10 Minuten (BitInfoCharts, 2022c)[74]. Bloxberg ist daher bei der Verarbeitungskapazität von Transaktionen als Blockchain selbst noch enorm skalierbar.

Das Besondere am PoE-Verfahren auf der Bloxberg-Blockchain liegt in dem Umstand, dass sich hier Wissenschaftsorganisationen gegenseitig ihren Forschungsoutput zertifizieren können. Zuvor stand einer einzelnen Wissenschaftsorganisation nur die Optionen offen, selbst innerhalb ihrer Organisation Existenznachweise anzulegen oder diese durch Dritte erstellen zu lassen bzw. eine Kombination von beidem. Durch die Nutzung

74 Wie in der vorangegangenen Evaluation von OpenTimestamps erörtert, hängt die Verarbeitungsdauer für Transaktionen auf der Bitcoin-Blockchain im Gegensatz zu Bloxberg jedoch von der Höhe der entrichteten Transaktionsgebühren ab.

des PoA-Konsensmechanismus bekommen Forschende ihre Existenznachweise auf der Bloxberg-Blockchain konsortial, also durch ein gesamtes Konsortium von renommierten Forschungsorganisationen, bestätigt. (Kleinfercher et al., 2020, S. 5.)

Die Zertifizierungs-dApp von Bloxberg basiert technisch auf einer Abspaltung (einem Fork) von Blockcerts[75], das speziell auf die Smart-Contracts-Funktionalität von Ethereum-basierten Blockchains ausgelegt ist[76]. Blockcerts ist ein offener Standard zur Ausstellung von Blockchain-basierten Zertifikaten, der in verschiedenen Branchen eingesetzt wird, etwa bei der Vergabe von Identitätsdokumenten, Zeugnissen oder Lizenzen (Blockcerts, 2022). Alle Komponenten sind Open Source über GitHub verfügbar[77] und werden dort weiterentwickelt.

In der aktuellen Fassung (v3) nutzt Blockcerts als Schema den W3C-Standard für Verifiable Credentials[78] im JSON-LD-Format in Verbindung mit einem Merkle-Tree-basierten Signaturverfahren (MerkleProof2019[79]). Nach dem GitHub-Repositorium[80] zu urteilen, wurde dieses Update auch bereits von Bloxberg adaptiert.

Bei der Nutzung des PoE-Dienstes (Research Object Certification) auf der Bloxberg-Blockchain wird ein Smart Contract mit folgendem Call ausgelöst:

```
createCertificate(address recipient, string tokenURI, string tokenHash)
```

Erstellt wird dadurch ein Research-Object-Certification-Token (ROC), das dem Ethereum-Standard ERC721 für Non-Fungible Tokens (NFTs)[81] entspricht. Die durch Bloxberg angepasste Spezifikation und das Schema ist im BLIP 2 Research Object Certification[82] niedergelegt (zur Erläuterung von BLIPs siehe weiter unten).

Die Empfängeradresse (recipient address) ist dabei die Adresse auf der Bloxberg-Blockchain, an die das ROC-Token über die dApp geschickt wird. Insofern beim Certify-Prozess nicht eine eigene Adresse angegeben wurde, ist dies eine durch Bloxberg vordefinierte Standard-Adresse, die speziell für diesen Vorgang angelegt wurde. Im Fall der Zertifizierung des Beispieldokuments ist dies über die automatisch vergebene Empfängeradresse 0x3fb704dfdb72fc06860d9f09124c30919488f13c (ResearchCertificate)[83] erfolgt. Durch die Ausführung des Contract Calls oben wird das Token der Adresse zugeordnet, sie besitzt also ab dem Zeitpunkt das Token.

Der tokenURI-String repräsentiert ein Feld, in dem ein Resolver für das Zertifikat festgelegt werden kann. Dieser ist bei der Research Certify dApp standardmäßig auf https://bloxberg.org gesetzt.

75 https://www.blockcerts.org
76 https://github.com/BlockcertsSmartContract
77 https://github.com/blockchain-certificates
78 https://www.w3.org/TR/vc-data-model/
79 https://w3c-ccg.github.io/lds-merkle-proof-2019/
80 https://github.com/bloxberg-org/cert-schema
81 https://ethereum.org/en/developers/docs/standards/tokens/erc-721/
82 https://github.com/bloxberg-org/blips/blob/master/blips/blip-2-researchcertificate.md
83 https://blockexplorer.bloxberg.org/address/0x3fb704dfdb72fc06860d9f09124c30919488f13c

Der tokenHash-String ist besonders bedeutsam für das PoE-Verfahren, weil dieser den Merkle Root übergeben bekommt, der im Verlauf des PoE-Prozesses über die zu attestierenden Dokumente generiert wurde. Für das Beispieldokument lautet dieser aa81ddb2ba33eba10e2c3912fff1604e320855df7b765c44bb78f8ea01939733.

Der Token-Hash findet sich neben dem Dokumentenhash (Cryptographic Identifier), der Transaktions-ID (Transaction ID) und dem Zeitstempel (Timestamp) auch im Research Object Certificate (siehe Abbildung 9) wieder, das Nutzer*innen am Ende des PoE-Prozesses als Attestierungsdatei im PDF-Format ausgegeben bekommen.


bloxberg

Research Object

Certificate

This bloxberg certificate serves as a proof of existence that the data corresponding to the cryptographic identifier were transacted on the **bloxberg** blockchain at the issued time.

Cryptographic Identifier

da3ba92c496d1b09b6342fad61b10f08cb309af82be6d47b3a59dabdcc60eaab

Transaction ID

0x90d560bcddc594e03ba5434ef3bdcbc7bfbe5f07cb157960f6ebd56bdef38c6a

Timestamp

2022-06-10T13:35:45.336347

Merkle Root

aa81ddb2ba33eba10e2c3912fff1604e320855df7b765c44bb78f8ea01939733

View the transaction at https://blockexplorer.bloxberg.org

Verify the certificate at https://certify.bloxberg.org/verify

Abbildung 9: Bloxberg Research Object Certificate

Im Testlauf mit dem Beispieldokument dauerte es wenige Sekunden, bis der Existenznachweis letztendlich auf der Bloxberg-Blockchain in einen Block geschrieben war.

Wie schon im Zertifikat (Abbildung 9) zu sehen, ist der Existenznachweis für die 379949eng.pdf (SHA256-Hash da3ba92c496d1b09b6342fad61b10f08cb309af82-be6d47b3a59dabdcc60eaab) auf der Bloxberg-Blockchain am 10.06.2022 um 13:35:45.336347 UTC mit der Transaktion 0x90d560bcddc594e03ba5434ef3bdcb-c7bfbe5f07cb157960f6ebd56bdef38c6a[84] erfolgt, die im Block 15831659 durch das Institut für Internet-Sicherheit[85] gemintet wurde.

84 https://blockexplorer.bloxberg.org/tx/0x90d560bcddc594e03ba5434ef3bdcb-c7bfbe5f07cb157960f6ebd56bdef38c6a/token_transfers

85 https://blockexplorer.bloxberg.org/blocks/15831659/transactions

Zur Verifizierung eines Existenznachweises kann dann das PDF-Zertifikat über die „Verify“-Schaltfläche in der dApp hochgeladen werden. Es erfolgt dann automatisch eine Formatvalidierung sowie ein Abgleich der Hashes, schließlich wird dann der Status des Zertifikats angezeigt (siehe Abbildung 10). Eine von dem Bloxberg-Web-Dienst unabhängige Möglichkeit zur Verifizierung von Zertifikaten bietet sich aufgrund der Blockcerts-Softwarebasis mit dem Blockcerts-Verifier, der auch in einer angepassten Variante über das Bloxberg-Coderepositorium beziehbar ist[86].

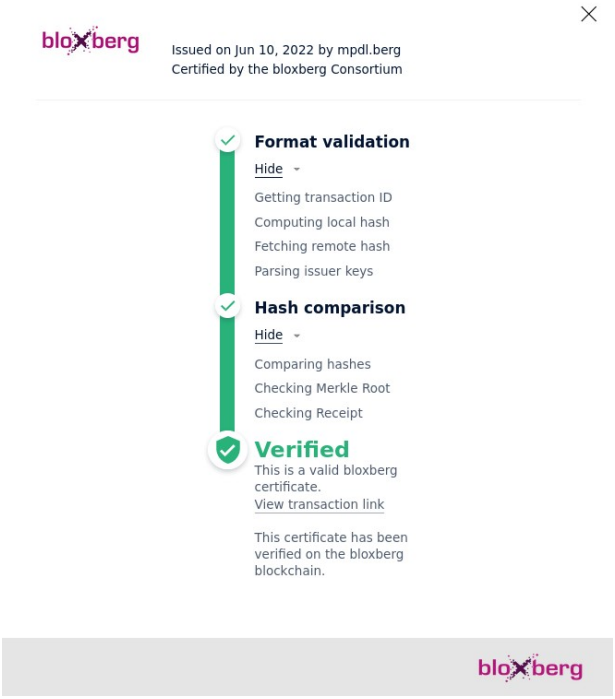


Abbildung 10: Verifizierung eines Bloxberg-Zertifikats

Der vollständige PoE-Ablauf aus der Nutzer*innenperspektive ist im Anhang B dokumentiert.

4.2.2 Anschlussfähigkeit an ein Blockchain-basiertes Open-Science-Ökosystem

Wie bereits in der Anfangsbemerkung zur Evaluation erwähnt, lassen sich im konstitutionellen Konzeptpapier von Bloxberg bereits einige Open-Science-Ansätze ausmachen. So heißt es dort eingangs als Ziel des Bloxberg-Konsortiums „to foster collaboration among the global scientific community, empowering researchers with robust, autonomous services that transcend institutional boundaries“ (Kleinfercher et al., 2020, S. 5).

Konkret manifestiert sich diese Intention etwa dadurch, dass die Bloxberg-Blockchain in jeder Hinsicht offen zugänglich ist. Einen zentralen Zugang zum Bloxberg-Projekt stellt für viele Forschende bzw. konventionelle Nutzer*innen sicherlich die Website bloxberg.org dar. Die Domain wurde ursprünglich durch die Max-Planck-Gesellschaft

86 https://github.com/bloxberg-org/blockcerts-verifier

registriert und diese ist auch seither Betreiberin der Website sowie der darüber angebotenen dApp-Web-Services (DomainTools, 2022). Wie bei Blockchain-Netzwerken üblich ist aber der Betrieb oder Zugang zur Blockchain aber nicht von einer solchen Web-Domain abhängig. Die Bloxberg-Blockchain kann von jedem offen eingesehen werden, etwa über den mittels der Web-Domain bereit gestellten Block Explorer[87] oder über den Betrieb eines eigenen non-Authority-Knotens, den jede Entität für sich selbst aufsetzen kann (Kleinfercher et al., 2020, S. 12).

Auch die Nutzung der Blockchain ist kostenfrei und steht jedem offen. Dies resultiert daraus, dass die Bloxberg-eigene Kryptowährung (bergs) über ein Faucet[88] an Interessierte ohne Gegenleistung ausgegeben und ansonsten nicht gehandelt werden, somit haben sie entgegen vieler Crypto-Coins und Tokens keinen Geldwert und werden ausschließlich zur Bezahlung der Transaktionsgebühren on-chain genutzt (Kleinfercher et al., 2020, S. 14).

Die Eigenschaft, Transaktionen zu validieren, also letztendlich neue Blöcke an die Blockchain zu hängen, obliegt jedoch allein den Validatorknoten (auch Authority Nodes genannt), die allein durch Mitglieder des Bloxberg-Konsortiums betrieben werden (Kleinfercher et al., 2020, S. 12–13).

Bloxberg versteht seine Blockchain im Kontrast zu den permissionless Blockchains als dezentraler angelegt und damit weniger beeinflussbar (Kleinfercher et al., 2020, S. 10). Während bei großen PoW-basierten Blockchains wie Bitcoin der Konsens durch einige wenige großer Mining-Pools kontrolliert wird (siehe OpenTimestamps Evaluation oben) sind auf der PoA-basierten Bloxberg-Blockchain dagegen mindestens 35 voneinander unabhängige Entitäten in der Gestalt von Wissenschaftsorganisationen zugegen, die als eigenständige Validatorknoten agieren. Für eine Übernahme des Bloxberg-Netzwerks mittels einer 51%-Attacke müssten sich also derzeit 18 Validatorknoten absprechen, während es bei Bitcoin nur die Ansprache von einigen wenigen dominanten Mining-Pools bräuchte, um das Netzwerk zu übernehmen.

Der Betrieb eines Validatorknotens steht jeder Wissenschaftsorganisation über die Mitgliedschaft im Konsortium offen (Kleinfercher et al., 2020, S. 15). Eine solche ist im Whitepaper definiert als „science organization, specifically academic, higher education and primarily publically funded research institutions“ (Kleinfercher et al., 2020, S. 18).

Die Mitgliedschaft im Konsortium kostet keinen Mitgliedsbeitrag, muss aber durch die Mehrheit der bestehenden Mitglieder per Vote on-chain bestätigt werden (Kleinfercher et al., 2020, S. 15). Jede Wissenschaftsorganisation darf nur einen Knoten betreiben, sodass die Machtverteilung ausgewogen bleibt. Der Validatorknoten muss dabei auf einem eigenen Server aufgesetzt und durch das eigene Personal administriert werden, sodass der ständige Betrieb gewährleistet ist. (Kleinfercher et al., 2020, S. 12, 16.) Es gibt regelmäßige informelle Treffen der Konsortiumsmitglieder. Jährlich wird sich zu ei-

87 https://blockexplorer.bloxberg.org

88 https://faucet.bloxberg.org, eine automatisierte Ausschüttung von Kryptowährung an eine bestimmte Blockchain-Adresse mit vorgeschalteten Anti-Spam-Maßnahmen.

nem Bloxberg Summit getroffen, auf dem größere Vorhaben wie etwa Änderungen am Governance-Modell besprochen werden (Kleinfercher et al., 2020, S. 19).

Nur dem Bloxberg-Konsortium angehörende Wissenschaftsorganisationen sind berechtigt, Änderungsvorschläge einzubringen und Entscheidungen über den Fortgang der Plattform zu treffen. Dies geschieht in der Form des Einbringens sowie der Abstimmung über Proposals und die Aufnahme von neuen Konsortiumsmitgliedern. Die Bloxberg Improvement Proposals (BLIPs) sind in der Analogie zur Bitcoin-Community (siehe Evaluation zu OpenTimestamps) ebenfalls öffentlich einsehbar[89] und die genauen Verfahrensweisen sind hier im BLIP 1 niedergelegt[90].

Um einen Anreiz dafür zu schaffen, dass Konsortiumsmitglieder regelmäßig am Governanceprozess teilnehmen, wurde das Abstimmungsrecht mit einem eigens dafür bestimmten Algorithmus (Bloxberg Decision Algorithm) verknüpft. Jedes Konsortiumsmitglied verfügt bei Entscheidungen über ein bestimmtes Stimmgewicht, das mit der erfolgten Stimmabgabe bei Abstimmungen steigt oder bei Nicht-Teilnahme sinkt. Es muss hierbei jedoch festgehalten werden, dass sich die elf Gründungsorganisationen bessere Ausgangsvoraussetzungen bei Abstimmungen eingeräumt haben, denn sie haben sich bereits mit der Bloxberg-Gründung ein initiales Stimmgewicht zugewiesen, während Neumitglieder bei null anfangen. (Kleinfercher et al., 2020, S. 15.)

Getroffene Entscheidungen bezüglich Neuzugängen oder Abgängen werden durch die ausführende Gewalt (Iron Throne) umgesetzt. Der Iron Throne wird seit der Gründung jährlich an ein Konsortiumsmitglied vergeben. (Kleinfercher et al., 2020, S. 16.) Im Gründungsjahr war dies die Max-Planck-Gesellschaft und diese hat auch auch nach der vierten Wiederwahl bis heute den Iron Throne inne (MPDL, 2022a). Die Prozesse zur Abstimmung über neue Mitglieder, den Iron Throne, die Änderung des Governance-Modells, Sanktionierungen und den Ausschluss sind fest definiert. Individuelle Forschende und andere konventionelle Nutzer*innen sind von der Governance ausgeschlossen, können die Blockchain aber frei nutzen. (Kleinfercher et al., 2020, S. 15–17.)

Die freie Nutzung beinhaltet auch die Möglichkeit für jede*n, auf der Bloxberg-Blockchain eigene Applikationen oder dezentrale Apps (dApps) zu betreiben (Kleinfercher et al., 2020, S. 11). Dafür steht eine offene interoperable REST-API[91] zur Verfügung und die Code-Repositorien der gesamten Bloxberg-Infrastruktur sind Open Source auf Guthub hinterlegt[92]. Die technischen Dokumentationen in den Bloxberg Code-Repositorien sind jedoch im Vergleich zu OpenTimestamps noch sehr fragmentär und es finden sich zu oft nur übernommene Dokumentationen der Ursprungssoftware, ohne dass Bloxberg-Spezifika vermerkt sind.

Das Bloxberg-Konsortium spricht sich aktiv für die Entwicklung von Apps aus, die der Scientific Community zugute kommen. Letztendlich sollen auf der Bloxberg-Blockchain

89 https://github.com/bloxberg-org/blips

90 https://github.com/bloxberg-org/blips/blob/master/blips/blip-1-purposeguidelines.md

91 https://blockexplorer.bloxberg.org/api_docs

92 https://github.com/bloxberg-org

basiert Anwendungen überall im Forschungsprozess unterstützend eingesetzt werden. Als potenzielle Anwendungsfälle für die Bloxberg-Blockchain werden im Whitepaper genannt:

- Schutz des geistigen Eigentums und von Daten allgemein
- Forschungsdatenmanagement
- Forschungsförderung
- Abbildung des Peer Review-Prozesses
- Identitätsmanagement für Forschende
- Blockchain-basierte Journals

(Kleinfercher et al., 2020, S. 23.)

Eine der ersten öffentlichen Implementierungen auf der Bloxberg-Blockchain ist der PoE-Dienst zur Zertifizierung und Verifizierung von Forschungsdaten. Die Research Data Certify & Verify dApp[93] zählt neben dem Faucet, Block-Explorer und Validator zu den zentralen Services, die als Kernelemente der Bloxberg-Infrastruktur betrachtet werden (Kleinfercher et al., 2020, S. 21–22). Hinter der Entwicklung und Betreuung der zentralen Services von Bloxberg steht hauptsächlich ein kleines Team bei der MPDL (MPDL, 2022b, Abschn. „Bereich Digitale Arbeitswerkzeuge“). Die Mitarbeitenden der über das Konsortium angeschlossenen Wissenschaftsorganisationen beteiligen sich unregelmäßig über Beiträge an verschiedenen Coderepositorien (GitHub, 2022b).

Genau wie OpenTimestamps kann das Research Data Certify Verfahren auf der Bloxberg-Blockchain auch mit großen Mengen von zu attestierenden Dateien umgehen, wie sie etwa bei Citizen-Science-Projekten aufkommen. Die eigentliche Verankerung auf der Blockchain geschieht hier innerhalb von Sekunden (siehe technische Eigenschaften oben), während diese bei OpenTimestamps (siehe Evaluation oben) mit Bitcoin mehrere Stunden dauern kann. Abgesehen von allgemeinen Blockchain-Statistiken lassen sich in der derzeitigen Implementierung von Bloxberg jedoch keine PoE-spezifischen Metriken abfragen.

Im Verlauf des PoE-Prozesses können Forschende optional Autor*innen- oder Gruppennamen, ihre E-Mail-Adresse und eine Kurzbeschreibung zu den Daten angeben (siehe Abbildung 11). Diese Angaben erscheinen aktuell aber nirgendwo im Klartext.

Es wurden bereits an verschiedener Stelle Proof of Concepts veröffentlicht, die zeigen, dass sich der PoE-Dienst der Bloxberg-Blockchain außerdem leicht mittels der zur Verfügung gestellten API in Forschungssoftware einbinden lässt. Wittek et al. (2020) demonstrierten etwa die Einbindung des Research-Certify-Verfahrens in das Softwaresystem MATLAB und Wolfram Blockchain Labs eine Erweiterung des Bloxberg-PoE-Dienstes um die Anbindung an IPFS (Woodard, 2021).

93 https://certify.bloxberg.org

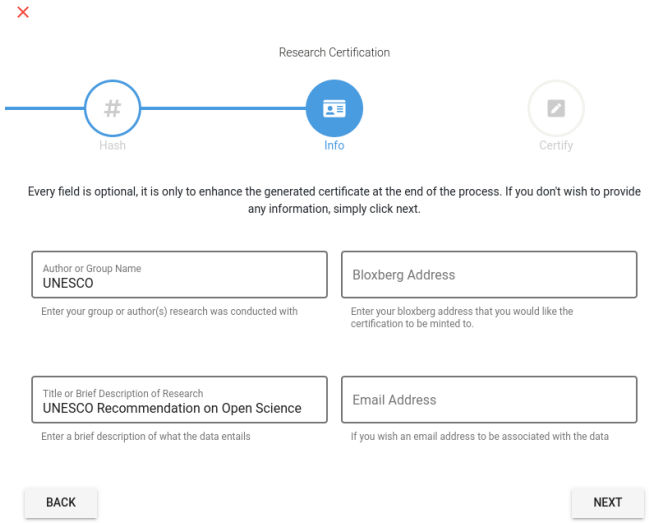


Abbildung 11: Optionale Datenangabe bei der Bloxberg-Zertifizierung

Bei der Nutzung des PoE-Dienstes werden seitens Bloxberg von den Nutzer*innen keine Kosten erhoben. Wie oben bereits erläutert, ist im Whitepaper festgehalten, dass auch die Cryptocoins der Bloxberg-Blockchain bewusst nicht gehandelt und Transaktionen kostenfrei sind. Seitens des Konsortiums ist daher eine Kommerzialisierung der zentralen Services und Prozesse auf der Blockchain, darunter die für PoE erforderlichen Mechanismen, aktuell ausgeschlossen.

Die Finanzierung der zentralen Bloxberg-Infrastruktur leistet seit der Gründung die Max-Planck-Gesellschaft, die wiederum vom deutschen Staat gefördert wird. Es wird sich auch auf Fördergelder beworben. Langfristig ist es das Ziel, aus diversifizierten Quellen Spenden zu erhalten. (Lawton, 2019.)

Für die Nutzung der Bloxberg-Blockchain sprechen laut dem Konzeptpapier allgemein, also unabhängig von einer Mitgliedschaft im Konsortium, folgende Anreize:

- die kostenfreie Nutzung
- das Netzwerk wird ausschließlich unterhalten durch Wissenschaftsorganisationen, die weltweit und demokratisch in einem Konsortium organisiert sind
- die konsortiale Trägerschaft stärkt die Sichtbarkeit aller auf der Bloxberg-Blockchain realisierten Applikationen innerhalb der Scientific Community

Als Anreize speziell für Konsortiumsmitglieder werden genannt:

- an der Gestaltung der Bloxberg-Infrastruktur und der Abstimmung über Regelungen der Governance und die Neumitglieder beteiligt zu sein
- ein starkes Zeichen zu setzen für dezentrale, unabhängige Services, die der Wissenschaft und der Scientific Community weltweit zu gute kommen

(Kleinfercher et al., 2020, S. 18.)

5 Ergebnisse der Evaluation

Wie der Gesamtbetrachtung der Evaluationsergebnisse (siehe Tabelle 2) zu entnehmen ist, liegen beide evaluierten PoE-Dienste bei der Erfüllung der Kriterien hinsichtlich der Anschlussfähigkeit an ein Blockchain-basiertes Open-Science-Ökosystem gleichauf.

Tabelle 2: Gesamtbetrachtung der Evaluationsergebnisse

Kriterien	**OpenTimestamps**	**Bloxberg Research Certification**
Offener Zugang	++	++
Zensurfreiheit	++	+
Identitäts- und Reputations-management	-	-
Erweiterbarkeit	++	++
Demokratische Beteiligung	++	+
Anreize	+	+
Workflow-Integration	+	++
Social Sharing	-	-
Finanzierung	+	+
Transparenz und Nachvollziehbarkeit	+	+
Citizen Science	++	++
Open Source	++	++
Ressourcenschonung	+	++
Metriken	+	-
Kompatibilität	+	++
Gesamtpunkte	19	19

Die Wertungszeichen in der Entscheidungsmatrix lassen sich dabei folgendermaßen aufschlüsseln:

- ++ = kann erfüllen (2 Punkte)
- + = kann nur bedingt erfüllen (1 Punkt)
- - = kann nicht erfüllen (0 Punkte)

Die argumentativen Grundlagen zur Vergabe der Wertungen sind im folgenden Abschnitt in einer zusammenfassenden Gegenüberstellung dargelegt.

5.1 Zusammenfassende Gegenüberstellung

Sowohl OpenTimestamps als auch Bloxberg erfüllen die Ansprüche an einen offenen Zugang, da sie ihre PoE-Dienste unter gleichen Bedingungen allen kostenfrei zur Verfügung stellen. Beide PoE-Verfahren sind trotz ihrer unterschiedlichen Implementierungsart problemlos skalierbar und können so etwa auch Existenznachweise en masse verarbeiten, wie es z.B. oft der Datenoutput von Citizen-Science-Projekten oder anderen datenlastigen Forschungsprojekten erfordert. Gleichzeitig sind die PoE-Methoden effizient und ressourcenschonend, indem sie eine schnelle Verarbeitung gewährleisten und die Hashes mehrerer Dateien aggregiert in einer Transaktion zusammengefasst auf der jeweiligen Blockchain nachweisen.

Aufgrund einer konsequenten Open-Source-Politik bei der Bereitstellung ihrer Code-Repositorien sind beide PoE-Dienste auch hinsichtlich der Erweiterbarkeit ein Vorzeigebeispiel. Bloxberg bietet jedoch durch die Bereitstellung der einfach zugänglichen interoperablen REST-API aktuell eine bessere Kompatibilität und konnte aus diesem Grund auch erwiesenermaßen bereits mit Forschungsoftware integriert werden. OpenTimestamps setzt in der Hinsicht die Auseinandersetzung mit der Bitcoin-spezifische RPC API sowie den Betrieb eines Bitcoin-Knotens voraus und kann noch keine dokumentierten forschungsspezifischen Anwendungsfälle vorweisen. Der Umstand, dass sich OpenTimestamps derzeit allein über Bitcoin betreiben lässt, bringt auch den Minuspunkt in Bezug auf den Ressourcenverbrauch mit sich, weil die Bitcoin-Blockchain aufgrund des PoW-Konsensmechanismuses im Betrieb einen enormen Energieverbrauch erzeugt. Auf der Bloxberg-Blockchain ist unter Einsatz von PoA bereits ein energiesparsames Betriebsmodell gegeben.

Der Grad an Zensurresistenz, den die beiden PoE-Dienste bieten, macht sich an den Konsensmechanismen und Governance-Modellen der dahinter liegenden Blockchains fest[94]. Im Fall von Bloxberg und OpenTimestamps mit Bitcoin ist es kontrovers, welche davon als mehr oder weniger dezentral gelten kann (siehe Diskussion zum Gegensatz zwischen permissionless und permissioned Blockchains weiter unten). Bitcoin wird an

94 Im November 2021 wurde bei Bloxberg ein Entwurf eines BLIPs zur Veränderung des Konsensmechanismuses eingebracht (GitHub, 2021). Inwiefern sich dieser Vorschlag bereits etabliert hat, konnte nicht abschließend festgestellt werden. Konkrete Änderungen sind auf der Blockchain aktuell nicht erkennbar, entsprechend kann diese Entwicklung im Rahmen dieser Arbeit nicht mehr berücksichtigt werden.

dieser Stelle ein höherer Grad an Zensurfreiheit eingeräumt, weil die Blockchain zum einen in ihrer über 13-jährigen Betriebszeit bisher keine Anzeichen von Zensur aufgewiesen hat und zum anderen aufgrund der breit gestreuten Nutzer*innenschaft als weniger parteiisch auch gegenüber der Scientific Community und ihren Belangen eingestuft werden kann. Bloxberg ist mit seiner dreijährigen Betriebszeit zu jung, als das bereits Aussagen bezüglich des praktischen Zensurpotenzials zu treffen wären und ob ein reiner Betrieb durch Akteure aus der Scientific Community zum Vor- oder auch Nachteil der Beeinflussbarkeit der Plattform sein kann. Ob darüber hinaus mit den derzeitigen Mitgliedern des Bloxberg-Konsortiums ein Querschnitt der Scientific Community abgebildet ist, bleibt ebenso fraglich.

Die Partizipation an Entscheidungsprozessen über den Fortgang der Plattform ist im Fall von Bloxberg jedoch durch die Voraussetzung einer Konsortiumsmitgliedschaft definitiv eingeschränkt. Im Sinne einer gleichberechtigten demokratischen Abstimmung innerhalb des Konsortiums gibt weiter der Fakt zu bedenken, dass sich die Gründungsorganisationen initial bessere Ausgangsvoraussetzungen bei Abstimmungen gesichert haben. Die Bitcoin-Community ist zwar wesentlich größer und fragmentierter mit zahlreichen unterschiedlichen Anlaufstellen, bietet aber prinzipiell jedem die Möglichkeit, sich zu beteiligen und mitzuentscheiden.

Keiner der PoE-Dienste verfügt über Möglichkeiten der Anbindung an Social Media bzw. Social-Sharing-Funktionalitäten. Möglicherweise sind solche Funktionen aber auch nicht erwünscht, etwa wenn überwiegend sensible Dokumente attestiert werden, die bewusst nicht an die Öffentlichkeit gelangen sollen. Aus dem selben Hintergrund könnte auch geschlossen werden, dass kein großes Augenmerk auf Metriken zu den Existenznachweisen gelegt wird. Allein OpenTimestamps bietet eine kleine Auswahl an Statistikwerten, die ausgegeben werden können. Die offenen Code-Repositorien würden sich hier aber dazu anbieten, dass Forschungseinrichtungen beauftragte Entwickler*innen solche Tools ergänzend programmieren lassen könnten.

Auch ein Identitäts- und Reputationsmanagement ist bei keinem der beiden PoE-Dienste vorzufinden. Während OpenTimestamps gemäß dem Prinzip der Wahrung der Privatsphäre bzw. Anonymität bewusst keine solche Funktion umsetzt, kann die offenbar aktuell noch unvollständig implementierte optionale Datenangabe im Attestierungsprozess bei Bloxberg aber als der Gang in diese Richtung gedeutet werden.

Die Angabe von optionalen Daten bei einem Existenznachweis kann auch in Bezug mit der Anforderung an die Nachvollziehbarkeit verschiedener Mitwirkenden bei der Erstellung eines Dokuments oder Datenobjekts ein gangbarer Weg sein. Die aktuell durch Bloxberg angebotene Lösung ist in der Hinsicht aber noch nicht ausgereift genug. OpenTimestamps bietet hier mit der Git-Integration eine Fertiglösung, die zumindest Forschende mit Git-Erfahrung zufrieden stellen sollte. Für eine völlige Offenlegung des Forschungsprozesses fehlt es aber bei beiden PoE-Diensten an den notwendigen Verarbeitungsprozessen und Darstellungsmöglichkeiten.

Hinsichtlich der Finanzierung verfolgen beide PoE-Projekte jeweils sehr bestimmte Strategien. Bloxberg baut auf die in der Forschung üblichen Fördergelder unter maßgeblicher Beteiligung einer großen Wissenschaftsgesellschaft[95]. OpenTimestamps finanziert sich ausschließlich aus Bitcoin-Spenden und Privatvermögen der Entwicker*innen. Allen den genannten Finanzierungsarten kann zum Nachteil ausgelegt werden, dass sie zu einseitig sind, entsprechend braucht es entweder eine universellere Spendenmethode oder insgesamt mehr Diversifizierung.

Bei den Anreizen stehen sich Bloxberg und OpenTimestamps diametral entgegen. Beide PoE-Dienste sind zwar kostenfrei nutzbar und negieren die Ausschüttung von werthaltigen Coins oder Tokens. Jedoch reserviert Bloxberg für sich als Gegenwert für eine Beteiligung am Projekt, ein Teil der Innovation innerhalb der Scientific Community sein zu können. OpenTimestamps macht sich allein dadurch lukrativ, dass es auf Basis der Bitcoin-Blockchain betrieben wird und somit jede*r Beteiligte*r mit der weltweit größten und beständigsten Blockchain interagiert. Beide müssten aber noch deutlich mehr Anreize bieten, um gerade die durch zentralisierte Lösungen großer Wissenschaftsverlage umworbenen Forschenden dauerhaft für ihre Services begeistern zu können.

5.2 Diskussion

In den nachfolgenden Abschnitten sollen nun noch einige wichtige Erkenntnisse hinsichtlich PoE-Diensten diskutiert werden, die sich im Rahmen der Evaluation von OpenTimestamps und Bloxberg ergeben haben.

5.2.1 Gegensatz zwischen permissionless und permissioned Blockchains

In der Evaluation dieser Arbeit standen sich in Bezug auf die zugrundeliegenden Infrastrukturen der PoE-Dienste zwei fundamentale Gegensätze gegenüber. OpenTimestamps verfolgt den permissionless Ansatz einer Infrastruktur, die möglichst losgelöst von Vertrauen funktioniert und gleichzeitig eine maximale Anonymität und Unabhängigkeit von zentralen Instanzen gewährleisten soll. Das Bloxberg-Projekt hingegen bietet einen permissioned Ansatz, der die Nutzung der Blockchain und des darauf angebotenen PoE-Dienstes in einen Zusammenhang mit der Reputation und dem Vertrauen in eine von Wissenschaftsorganisationen konsortial betriebene Infrastruktur stellt.

Welches Governance-Modell nun mit einem höheren Grad an Dezentralisierung einher geht, ist kontrovers und kann oft erst aus der Praxis heraus eindeutig bestimmt werden. Bakos et al. (2021, S. 20–22) weisen in der aktuellen Diskussion darauf hin, dass permissionless Blockchains zwar theoretisch eine Dezentralisierung anstreben, die faktische Kontrollausübung im Betrieb sich dann aber oft zentralisiert, weil dieser Prozess bei einem solchen Governance-Modell letztendlich auf Basis individueller Entscheidungen entsteht. Die Autor*innen argumentieren weiter, dass permissioned Blockchains

95 Im Mai 2022 wurde auf dem vierten Bloxberg Summit die Einführung von Tokenomics beschlossen, um die nachhaltigen Finanzierung der Infrastruktur sicherzustellen (MPDL, 2022a). Die konkreten Auswirkungen dieser Entscheidung sind derzeit noch nicht absehbar, daher können diese im Rahmen dieser Arbeit nicht mehr berücksichtigt werden.

eine bessere Grundlage für dezentralisierte Governance bieten können, wobei hier aber besonders auf die Ausgestaltung des Gatekeepings geachtet werden muss.

Eine korrespondierende Beobachtung mit den Thesen von Bakos et al. (2021) konnte auch diese Arbeit im Rahmen der Evaluation der beiden PoE-Dienste und ihrer zugrundeliegenden Blockchain-Infrastrukturen Bitcoin und Bloxberg machen. Getroffene Entscheidungen der Bitcoin-Community bedürfen am Ende immer die konsensuale Ausführung durch die Validatorknoten (Miner), deren Macht sich aber zeitweise bei einigen wenigen Mining-Pools konzentriert und daraus eine Anfälligkeit für 51%-Attacken resultiert. Solche 51%-Attacken sind gerade in den letzten Jahren zunehmend zu einer realen Bedrohung für permissionless Blockchains geworden, die Fälle betroffener Netzwerke häufen sich (Attah, 2020).

Wohingegen bei den großen etablierten permissionless Blockchains wie Bitcoin mit hoher Wahrscheinlichkeit davon ausgegangen werden kann, dass der Weiterbestand aufgrund der breiten Beteiligung vieler Branchen und Interessengruppen über längere Zeit gesichert ist, müssen im Fall von permissioned Blockchains die Akteure dahinter hinsichtlich ihrer Vertraulichkeit und Verlässlichkeit, also ihrem dauerhaften Commitment und den für die Blockchain allokierten Ressourcen, genau betrachtet werden. Die Evaluation dieser Arbeit zeigt, dass Bloxberg diese Eigenschaften aufgrund seiner Transparenz und dem konsortialen Betrieb durch etablierte Wissenschaftsorganisationen für sich reservieren kann. Ob das Bloxberg-Governance-Modell in seiner aktuellen Form aber als dezentralisiert bezeichnet werden kann, bleibt fraglich. Nach Bakos et al. (2021, S. 22) spielt es hierbei vor allem eine Rolle, wie die existierenden Validatorknoten als Gatekeeper mit der Vergabe und dem Entzug der Validatoren-Eigenschaft von neu hinzukommenden Knoten umgehen.

Auch wenn das Governance-Modell von Bloxberg demokratische Züge hat, könnte das Missverhältnis in der Stimmgewichtung zwischen Gründungsorganisationen und Neumitgliedern im Konsortium als ein undemokratischer Einschnitt in der Ausübung des Stimmrechts gewertet werden. Bei vorausgesetztem korrekten Stimmverhalten baut sich das Missverhältnis des Stimmgewichts zwischen den Neumitgliedern, die bei null anfangen müssen, und den Gründungsorganisationen sukzessive aus. Auch trotz einer Maximalgrenze des Stimmrechts sind es die Gründungsorganisationen, die das Maximum als erste erreichen. Dies könnte möglicherweise im weiteren Verlauf der Zeit bei Abstimmungen zu einer unüberwindbaren Grunddominanz durch die Gründungsorganisationen führen.

Auch in Hinsicht auf den Konsensmechanismus unterscheiden sich die beiden evaluierten PoE-Dienste fundamental. OpenTimestamps setzt mit der Bitcoin-Blockchain als maßgebliche Basis auf den PoW-Konsensmechanismus, während Bloxberg und seine darauf basierenden Dienste PoA nutzen.

Am Beispiel von Bitcoin und Ethereum zeigt sich seit den letzten Jahren deutlich, dass der Betrieb von auf dem PoW basierenden Blockchain-Netzwerken mit einem enormen Energieverbrauch einher geht, sobald das Netzwerk eine gewisse Größe und Last er-

reicht hat (Cambridge Centre for Alternative Finance, 2022). Die Konsequenz daraus ist ein hoher CO2-Ausstoß und ein enormer Hardwareverschleiß, der sich wiederum auf das Weltklima und den Weltmarkt auswirkt und sich gerade seit den letzten Jahren zunehmend in der Weltgemeinschaft spüren lässt.

Momentan gibt es seitens der Europäischen Union (EU) Pläne, im Zuge der Durchsetzung von Maßnahmen zur Reduzierung der CO2-Emissionen den Handel und das Mining von PoW-basierten Kryptowährungen bzw. Crypto-Coins zu verbieten oder zu regulieren (Fanta, 2022). Es muss also auch davon ausgegangen werden, dass ein solches Verbot Auswirkungen auf PoE-Dienste haben wird, die auf PoW-Blockchains basieren.

Seitens der Bitcoin-Community wird überwiegend argumentiert, dass PoW der einzige Konsensmechanismus ist, der das Netzwerk zensurfrei halten könne und die Auswirkungen auf die Umwelt zum Erhalt dieser Freiheit in Kauf genommen werden müsse (Blockchain Bird, 2022). Die Ethereum-Community wiederum bereitet seit mindestens zwei Jahren aktiv den Wechsel ihres Blockchain-Netzwerks auf den ressourcenschonenderen PoS-Konsensmechanismus vor, der aber bis dato nicht umgesetzt wurde (Ethereum.org, 2022b).

Die aktuelle Forschung macht hierzu auch noch einmal deutlich, dass der hohe Energieverbrauch ein Blockchain-Netzwerk-spezifisches Problem ist und nicht der Blockchain-Technologie generell angelastet werden kann (Sedlmeir et al., 2020). In diesem Bezug ist Bloxberg positiv herauszustellen, weil das Netzwerk bereits mit dem PoA-Konsensmechanismus zumindest in der Hinsicht des Energieverbrauchs deutlich ressourcenschonender betrieben wird und auch bei vergleichbarer Größe deutlich weniger Energie verbrauchen würde als Bitcoin oder Ethereum.

Jedoch sind alle auf der Blockchain-Technologie basierende Netzwerke auf eine gewisse Weise ressourcenverschwendend, da überall Daten redundant gespeichert werden müssen. Auf der Bitcoin- und Bloxberg-Blockchain müssen die angeschlossenen Knoten jeweils eine Kopie der Blockchain vorhalten, die im Fall von Bitcoin, wie bereits dargelegt, aktuell über 400 GB groß ist. Hier kann eine zentrale Lösung ressourcenschonender sein, in der Realität werden jedoch gerade bei groß angelegten zentralen Systemen ebenfalls die Daten auf viele verschiedene Server verteilt. In puncto Geschwindigkeit bei der Auslieferung von Inhalten haben zentral angelegte Systeme momentan einen Vorteil. Bei einem dezentralen Netzwerk steht dies immer im Zusammenhang, wie viele Knoten einem dezentralen Netzwerk permanent zur Verfügung stehen und ob diese geografisch adäquat verteilt sind, was wiederum von der Etablierung des Projekts und der Partizipationswilligkeit von Knoten-Betreibenden abhängt.

Festhalten lässt sich jedenfalls, dass abgesehen von den fundamentalen Eigenschaften einer Blockchain, die nicht geändert werden dürfen, weil sie sonst das Verfahren gefährden (siehe Grundlagen-Kapitel), etwa die Auswirkungen auf das Klima durch technische Eingriffe (wie den Wechsel des Konsensmechanismuses oder der mehrheitlichen und nachweisbaren Umstellung der Knoten auf erneuerbare Energien) und

auch politische Intervention (z. B. durch Regulierung) verändert werden können. Skeptiker weisen jedoch darauf hin, dass neben den Auswirkungen auf das Klima auch die politischen, sozialen und ökonomischen Implikationen hinter vielen Blockchain-Projekten problematisch sind: etwa der Anspruch einer Tokenisierung[96] von allem oder die Abwertung von Vertrauen als einen Grundpfeiler der Gesellschaft (Tante, 2022). Eine weitere Auseinandersetzung kann aber aufgrund ihrer Komplexität nicht Bestandteil der vorliegenden Arbeit sein.

5.2.2 Defizite in Bezug auf die Attestierung bei PoE-Diensten

Im Rahmen der Evaluation ließen sich auch einige Schwachpunkte von PoE-Diensten identifizieren, dies betraf zum einen speziell den Prozess der Attestierung.

Ein besonders ernstzunehmendes Problem liegt im Verlust der Attestierungsdatei oder des dazugehörigen attestierten Dokuments. Im Fall von OpenTimestamps stehen Nutzer*innen beim Verlust der Attestierungsdatei vor dem kritischen Problem, dass damit die Existenznachweise nicht mehr reproduziert werden können, weil die dafür notwendigen Herleitungssequenzen fehlen. Aufgrund des Binärformats einer .ots Attestierungsdatei lässt sich diese auch bei vorliegenden Teilinformationen wie Transaktionshash oder Merkle-Tree mit an Sicherheit grenzender Wahrscheinlichkeit nicht rekonstruieren. Auch bei Bloxberg lässt sich der Verifizierungsprozess ohne vorliegendes PDF-Zertifikat nicht mehr anstoßen. Das zugrundeliegende Blockcerts-Framework würde aber möglicherweise mittels des JSON-LD Basisformats eine Rekonstruktion anhand Teilinformationen zulassen. Grundsätzlich sind aber in keinem der beiden evaluierten PoE-Dienste Mechanismen einprogrammiert, die einen solchen Verlust der Attestierungsdatei berücksichtigen. Es besteht also keine Möglichkeit, eine frühere Attestierungsdatei nochmals zu erhalten. Dies nicht anzubieten, ergibt im Kontext der Datensicherheit aber Sinn, da eine solche Datei zu diesem Zweck etwa dauerhaft auf einem Server gespeichert werden müsste.

Geht das attestierte Dokument selbst verloren, ist das ein grundsätzliches Problem bei allen PoE-Diensten, da diese zum Schutz des Inhalts vor der Einsicht Dritter nie das Dokument selbst speichern, sondern nur den Dateihash. In der Praxis kann es auch oft vorkommen, dass nach dem getätigten Existenznachweis unbewusste Veränderungen des Dokuments geschehen, etwa durch die Funktion des automatischen Abspeicherns bei Office-Dokumenten, und sich dadurch der ursprüngliche Dokumentenhash ändert. Es muss also sichergestellt sein, dass die Originaldatei dauerhaft und bit-genau wie zum Zeitpunkt des Existenznachweises vorgehalten wird. Hierfür empfiehlt es sich, entweder mit Versionierungssystemen zu arbeiten oder die Dokumente in dezentrale manipulationssichere Speichersysteme einzuspeisen (siehe dazu weitere Forschungsansätze im Abschnitt „Fazit und Ausblick“).

Ein weiteres Problem liegt in der unabhängigen Verifizierung einer Attestierung. Um eine solche unabhängig von einer Mittelsinstanz direkt auf der Blockchain vornehmen

96 Gemeint ist eine finanzielle Verwertung in Gestalt von Crypto-Coins oder Tokens.

zu können, braucht es sowohl bei OpenTimestamps als auch bei Bloxberg den Betrieb eines eigenen Netzwerk-Knotens. Diese Hürde geht im Fall von OpenTimestamps noch mit einer enormen Ressourcenverschwendung einher, weil die Größe der vorzuhaltenden Bitcoin-Blockchain über 400 GB beträgt, die in jedem Fall mindestens einmal komplett heruntergeladen werden muss, selbst wenn ein speicherplatzsparender Knoten (Pruned Node) aufgesetzt wird.

Ein klares Defizit, das vor allem bei der Bitcoin-Blockchain wegen des PoW-Konsensmechanismuses zum Tragen kommt, ist der unkalkulierbare Zeitverzug bis zur Verzeichnung auf der Blockchain. Über OpenTimestamps kann es einen schwer vorab einzuschätzenden Zeitraum (aktuell meist mehrere Stunden) dauern, bis der Existenznachweis tatsächlich über die Blockchain nachgewiesen ist, während Bloxberg dies höchst berechenbar in Sekunden abwickelt.

Auch in Bezug auf die Beigabe von individuellen Metadaten während des Attestierungsprozesses sind die evaluierten PoE-Dienst höchst defizitär. In OpenTimestamps können überhaupt keine individuellen Metadaten mitgegeben werden, auf Bloxberg sind die optionalen Daten aus der Attestierung nicht offen einsehbar.

5.2.3 Sicherheitsbedenken in Bezug auf PoE-Verfahren

Des Weiteren sind auch allgemeine Sicherheitsbedenken in Bezug auf das PoE-Verfahren zu diskutieren.

Blockchains sind wie alle auf Hashing-Methoden basierende Verfahren Angriffsvektoren wie der Hash-Inversion oder -Kollision ausgesetzt. Angriffe werden jedoch als eingeschränkt möglich beschrieben, da die Blockchain-Technologie nur in einem vergleichbar geringen Umfang auf Hashing zurückgreift. (Swan, 2015, S. 40.) Das von vielen etablierten Blockchain-Projekten genutzte SHA-256-Verfahren ist aktuell ein Industriestandard und wird gemäß der technischen Richtlinie „Kryptografische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (Bundesamt für Sicherheit in der Informationstechnik) als für die nächsten zehn Jahre sicher eingestuft. Hierbei sollte sich noch vergegenwärtigt werden, dass ein Bruch von SHA-256 nicht nur Auswirkungen auf Blockchains, sondern auf ganze Industriesektoren und die gesamte Sicherheitsarchitektur des Internets (z. B. SSL/TLS) hätte. (Pohlmann, 2019, S. 509.) Obwohl es bislang keine praxisrelevanten Angriffe gab, wurde 2015 als Nachfolger das Keccak-Verfahren unter dem Namen SHA-3 standardisiert (Manz, 2019, S. 102). Keccak kommt auch zunehmend in Blockchain-Projekten zum Einsatz.

In der Post-Quanten-Kryptografie werden derzeit neue kryptografische Standards entwickelt, die eine Resistenz gegen den Einsatz von Quantencomputern zum Brechen von Hashes aufweisen, und langfristig auch durch die Blockchain-Technologie adaptiert werden müssen. Mit Blockchains ist ein Umstieg auf neue kryptografische Verfahren technisch möglich, auch wenn dies etwa zur Folge hat, dass Blockchain-Teilnehmende sich neue Adressen generieren müssen. (Pohlmann, 2019, S. 84–86, 510.) Essenziell für die Resilienz von Blockchains erscheint die Möglichkeit des Rehashings auf

stärkere Verfahren (DIN/TS 31648, 2021, S. 23–24) und allgemein die Berücksichtigung von Handlungsempfehlungen bezüglich der Migration zu Post-Quanten-Kryptografie (Bundesamt für Sicherheit in der Informationstechnik, 2020, S. 6–8).

Unabhängig von der Blockchain wären speziell PoE-Verfahren auch von Angriff auf Hashing-Algorithmen an sich betroffen. Seitens PoE-Entwickler*innen wird das aber als unwahrscheinlich eingeschätzt, selbst in Bezug auf die Nutzung bereits überholter Hashingverfahren wie SHA1 (Todd, 2017c). Hierzu kann auch festgehalten werden, dass die evaluierten PoE-Dienste OpenTimestamps und der Bloxberg Research Certification Service bei der Attestierung beide auf das momentan als sicher eingestufte SHA256-Verfahren zurückgreifen.

Aufgrund der Tatsache, dass die Nutzung von PoE-Diensten sehr günstig ist, stellt sich wie auch allgemein bei allen Zeitstempel-Diensten das Problem des Brute-Force-Timestampings. Bestimmte Akteure könnten systematisch von Inhalten Existenznachweise erstellen, um sich später zu einem bestimmten Zweck oder eigenen Nutzen auf nur eine kleine Auswahl von diesen berufen zu können. Dies kann zum Beispiel in Hinsicht auf Vorhersagen oder Prognosen von bestimmten Ereignissen, in der Forschung etwa in der Form von Messdaten, problematische Implikationen mit sich bringen.

So gesehen hat PoE aktuell dasselbe Double-Spending-Problem, das eigentlich durch die initiale Erfindung von Bitcoin bereits gelöst ist (siehe Grundlagen-Kapitel). PoE kann nicht die Einzigartigkeit eines Dokuments beweisen. Für den selben Dokumentenhash lässt sich beliebig oft ein Existenznachweis ausstellen. Insofern das Dokument also nicht im Vorhinein in einem Zusammenhang mit einer Identität gesetzt werden kann (z. B. durch die Nennung des Personennamens im Dokument oder durch eine digitale Signatur), wäre diejenige Person, die zuerst den Existenznachweis erstellt, möglicherweise unberechtigterweise im Vorteil gegenüber allen Personen, die dies nach ihr tun. Im Forschungskontext könnte das zu einem Problem werden, wenn an einer Arbeit mehrere Personen beteiligt sind und Dissens bzw. Misstrauen bezüglich der weiteren Verwertung herrscht. Auch in diesem Kontext wären Lösungsansätze wie der Einsatz von Notaren beim Betrieb eines PoE-Dienstes (Härer & Fill, 2020, S. 4–5) oder rein digitale Lösungen wie z. B. Single-Use-Seals (Todd, 2017b) oder Research Object Chain Links (Wittek et al., 2021) zu diskutieren.

In dem Zusammenhang sei abschließend auf einen häufigen Fehlschluss im Zusammenhang mit Existenznachweisen hingewiesen: Der Nachweis über die Existenz eines Inhalts beweist nicht oder trifft keine Aussage darüber, ob der Inhalt auch zutrifft bzw. korrekt ist. In einem Zeitalter, das geprägt ist durch Desinformation, in diesem Kontext vor allem jene, die sich durch die bewusste Manipulation von Daten auszeichnet, sollte sich das stets bewusst gemacht werden.

6 Fazit und Ausblick

Die Evaluation der vorliegenden Arbeit zeigt, dass aus technisch-infrastruktueller Hinsicht beide PoE-Dienste gleichauf für den Einsatz als Teil eines Blockchain-basierten Open-Science-Ökosystems geeignet sind, wenn auch beim Vertrauensgrad in die zugrundeliegende Infrastruktur zwischen permissioned und permissionless abgewägt werden muss.

OpenTimestamps zeichnet sich als ein ausgereifter generischer PoE-Dienst aus, der über die Wissenschaft hinaus alle Belange der Erstellung von Existenznachweisen abdecken will, indem er seinen Nutzer*innen ein Maximum an Unabhängigkeit und Anonymität bietet, das nur ein Minimum an Vertrauen in den Dienst erfordert. Solange OpenTimestamps aber de facto untrennbar von der Bitcoin-Blockchain bleibt, muss sich der PoE-Dienst an den selben Maßstäben messen lassen wie Bitcoin selbst. Insofern das Bitcoin-Netzwerk und dahinter die Community also den jetzigen Kurs beibehält, kann auch die Nutzung von OpenTimestamps nur in Ausnahmefällen zu rechtfertigen sein.

Der durch Bloxberg explizit für Forschende gestaltete Research-Object-Certification-Dienst kann sich im starken Kontrast zu OpenTimestamps auf eine vertrauenswürdige Infrastruktur stützen, die durch reputable Wissenschaftsorganisationen konsortial getragen wird und damit besser anknüpft an die Verfasstheit der Scientific Community, die maßgeblich auf Reputation und Transparenz der beteiligten Akteure baut. Bloxberg ist mit seiner Infrastruktur im Vergleich das geringere Übel und hat mehr Potenzial für Veränderung, wie es sich an aktuellen Beschlüssen des Konsortiums ablesen lässt. Die Umsetzung des Research Certification Services mit Blockcerts ist nach aktueller Einschätzung eine zukunftstaugliche Entscheidung, weil sie auf den W3C-Standard für Verifiable Credentials setzt. Blockcerts kann im Gegensatz zu OpenTimestamps auch für sich reservieren, eine PoE-Lösung zu sein, die momentan wirklich auf mehreren und technologisch unterschiedlichen Blockchains betrieben wird.

Des Weiteren konnten im Rahmen der Evaluation einige Defizite der PoE-Dienste und potenzielle Angriffsvektoren auf das PoE-Verfahren herausgearbeitet werden, die hinsichtlich einer Entscheidungsfindung auch zu berücksichtigen sind.

Wie diese Arbeit in jedem Fall zeigen konnte, bieten beide PoE-Dienste und die dahinter liegenden Plattformen aufgrund ihrer offenen Infrastruktur und des offen gelegten Quellcodes für jede interessierte Person aus dem Forschungsumfeld die Gelegenheit, sich selbst einen Einblick zu verschaffen und dann letztendlich selbst zu entscheiden, welche davon sich als eine Lösung für das Erstellen von Existenznachweisen eignet.

6.1 Weitere Forschungsansätze

Hinsichtlich der Implementierung eines auf Open Science ausgerichteten PoE-Dienstes stellen sich in der Praxis noch viele Fragen. Zum Beispiel: Wie lässt sich das Erstellen von Existenznachweisen bei dynamischen Inhalten am besten umsetzen? Im Forschungsprozess entstehen gewöhnlicherweise zu vielen verschiedenen Zeitpunkten viele verschiedene Varianten von Dokumenten und Datasets oder auch Websites. Können Blockchain-basierte Methoden (z. B. Smart Contracts oder verteilte Dateisysteme) genutzt werden, um das PoE-Verfahren bei sich ständig verändernden Inhalten zu automatisieren, reichen stattdessen konventionelle Versionierungssysteme (z. B. Git) aus oder braucht es eine Kombination?

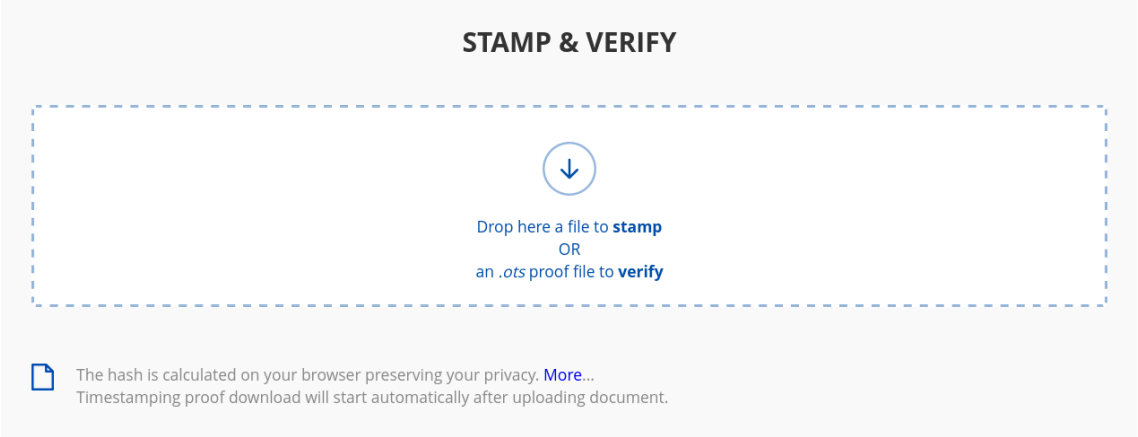
Es bleibt auch offen, inwiefern PoE-Dienste oder PoE-Verfahren verlässlich die Autorenschaft von Dokumenten nachweisen können oder sollen. Die Integration von PoE mit einer Identitäts-basierten Art der Nutzung geht mit einem deutlich höheren Grad an Komplexität an die Umsetzung einher, deswegen ist sie aktuell selten vorzufinden. Hinsichtlich der Gewährleistung von Dezentralität ist es hierbei auch fraglich, ob an dieser Stelle auf eine Anbindung an zentrale IDM- (Identity Management), SSO- (Single Sign-On) oder Identifikatorensysteme wie etwa ORCID zurückgegriffen werden soll oder sich auch kryptografisch verifizierbare Methoden wie PGP (Pretty Good Privacy) oder DIDs (Decentralized Identifiers) eignen (Bach, 2021).

Um den neueren Entwicklungsansätzen Rechnung zu tragen, sollte auch noch das InterPlanetary File System (IPFS) im Kontext einer Open-Science-Infrastruktur näher untersucht werden. IPFS nutzt wie die Blockchain-Technologie bestimmte Prinzipien der Kryptografie und des Trusted Timestamping, um daraus ein dezentral verteiltes Dateisystem mit einem globalen Namensraum auf Basis einer verteilten Hashtabelle (Distributed Hash Table) zu realisieren. Aufgrund seiner Komplexität konnte es letztendlich keinen Eingang in die Evaluation dieser Arbeit finden.

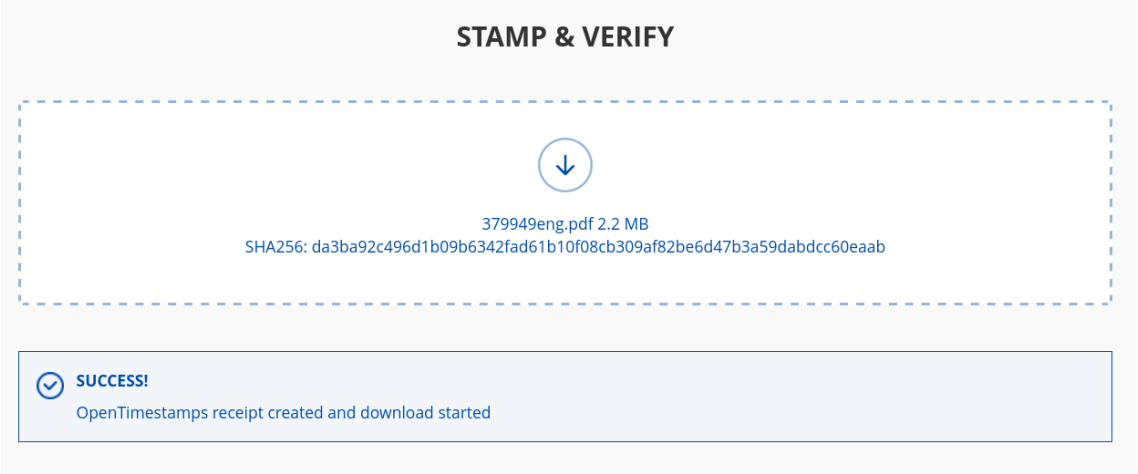
IPFS könnte einen signifikanten Bestandteil eines PoE-Verfahrens ausmachen, wenn eine manipulationssichere off-chain Datenhaltung in Betracht gezogen werden soll. Dies kann aus Gründen des Datenschutzes bzw. regulatorischer Vorgaben (siehe Abschnitt zu PoE-relevanten Normen in Deutschland im Grundlagen-Kapitel, dort speziell die Ausführungen zur DIN/TS 31648) oder auch zum Zwecke eines bewussten Zurückhaltens von Daten (Moratorium, siehe Punkt 11 der Kriterien für ein Blockchain-basiertes Open-Science-Ökosystem) geschehen. Vorstellbar wären im Zusammenhang mit der Anbindung an ein solches dezentrales Speichersystem entweder das Betreiben eines privaten IPFS-Netzwerks durch eine oder mehrere Wissenschaftsorganisation(en) (die Knoten stellen hierbei ausschließlich vertrauenswürdige Entitäten in einer kontrollierten Umgebung), in dem sowohl Dokumente als auch Attestierungsdateien gehalten werden, oder das Einspeisen ausschließlich bestimmter Dateien, z. B. nur der Attestierungsdateien, in das öffentliche IPFS-Netzwerk bei gleichzeitiger Dateihaltung sensibler Inhalte mittels anderer Speichermethoden auf Seiten der Forschungseinrichtungen (lokaler Fileserver, private Cloud oder physikalische Datenträger).

Darüber hinaus wäre es sicherlich ein Erkenntnisgewinn, detailliert herauszuarbeiten, inwiefern und unter welchen Bedingungen PoE-Dienste mit der DSGVO und anderen Datenschutzanforderungen oder auch den Anforderungen an die IT-Sicherheit konform sind. Das BSI etwa hat bereits seine Empfehlungen bezüglich den IT-Sicherheitsvoraussetzungen bei Blockchain bzw. DLT in verschiedenen Papieren publiziert. Diese haben auch bereits in die hier behandelte DIN/TS 31648 (siehe Abschnitt „PoE-relevante Normen in Deutschland“) Eingang gefunden.

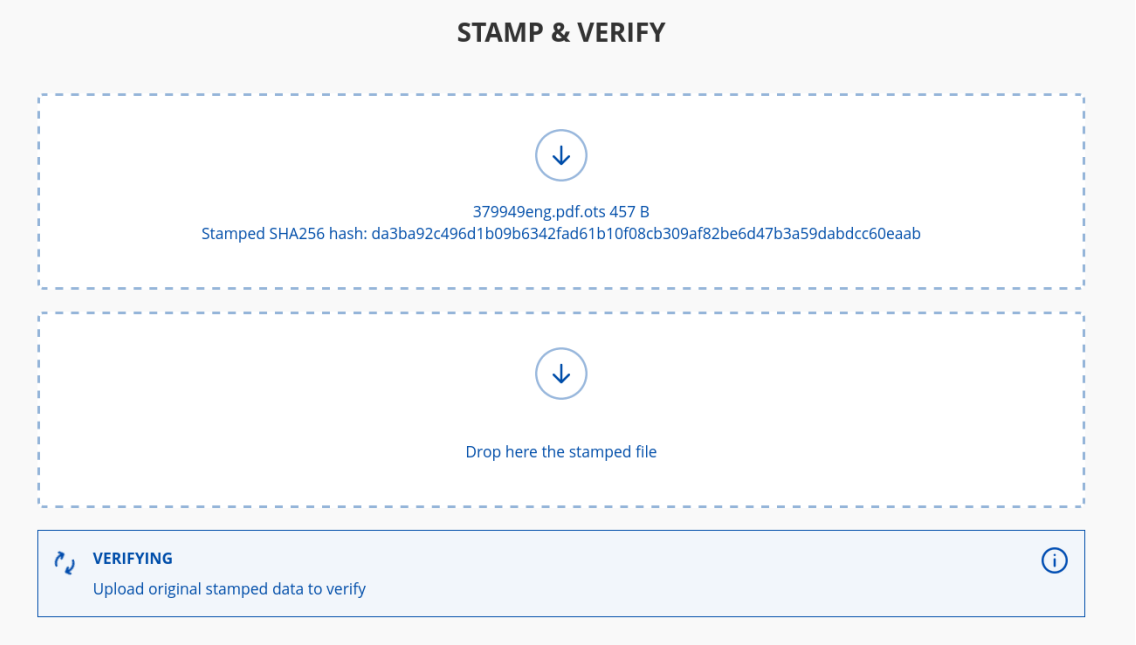
Anhang A: Attestierung des Beispieldokuments mit OpenTimestamps



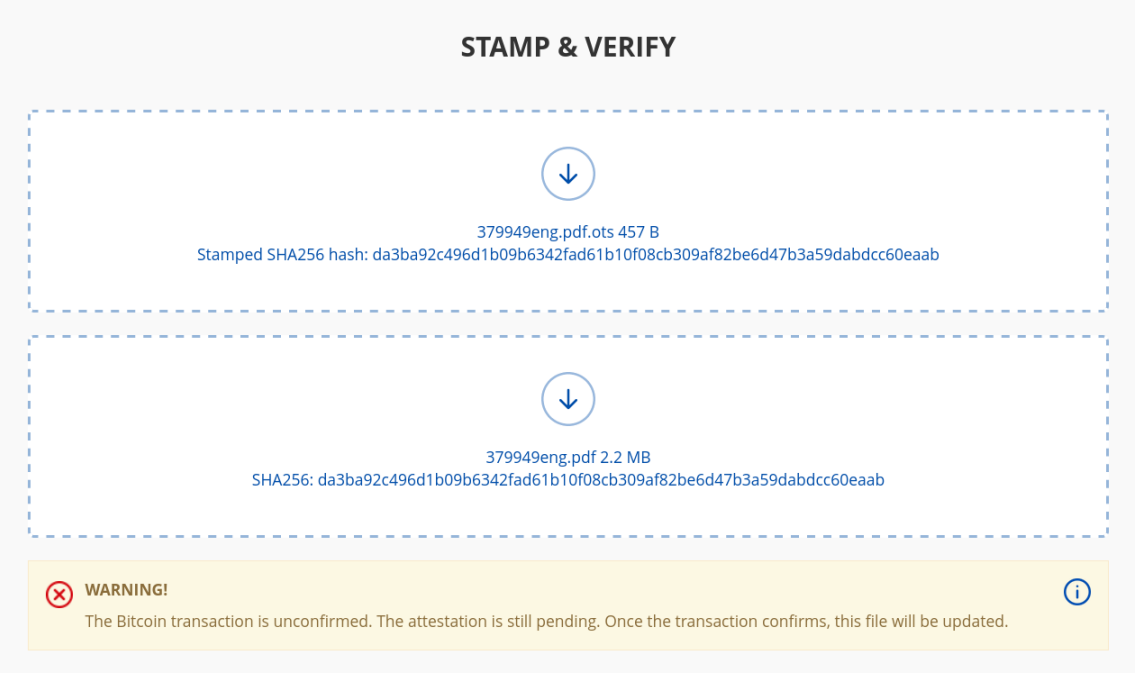
1. Zuerst wird das zu attestierende Dokument in das „Stamp & Verify“-Feld gezogen oder über den Dateiauswahl-Dialog gewählt.



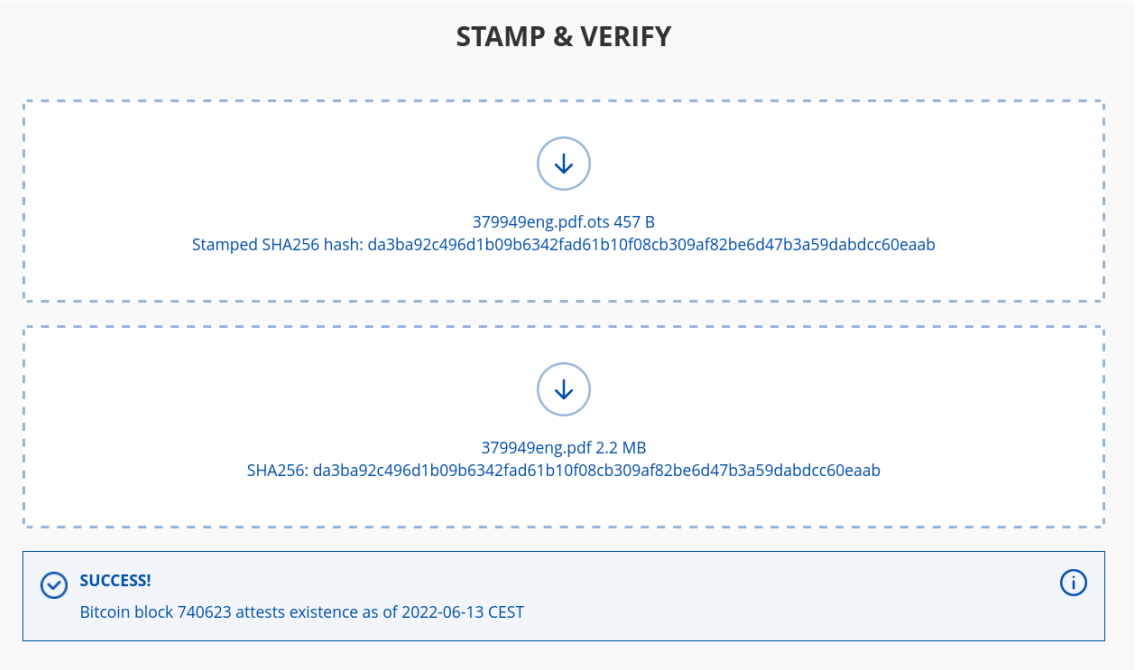
2. OpenTimestamps generiert dann den SHA256-Hash der Datei und die vorläufige .ots Attestierungsdatei wird sofort als Download über den Browser ausgegeben.



3. Zur Verifizierung muss sowohl die Attestierungsdatei als auch das dazugehörige Dokument über das „Stamp & Verify“-Feld ausgewählt werden.

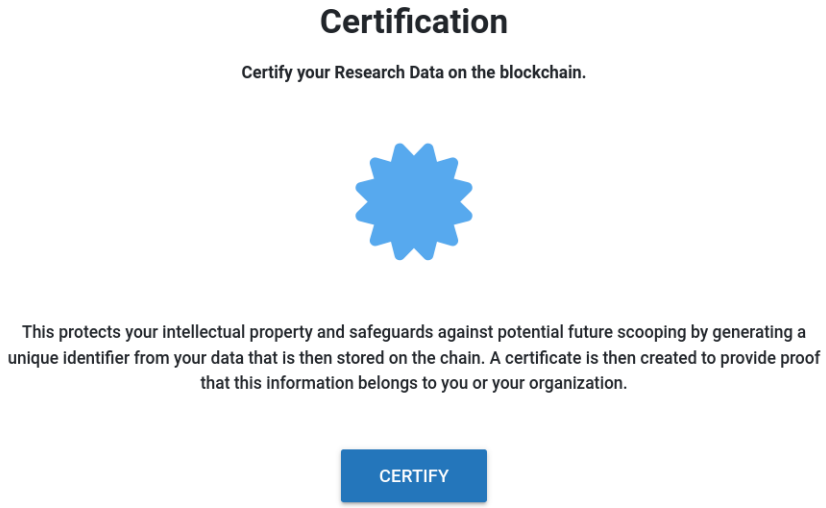


4. Ist die Attestierung auf der Blockchain noch nicht erfolgt, erscheint eine entsprechende Meldung.

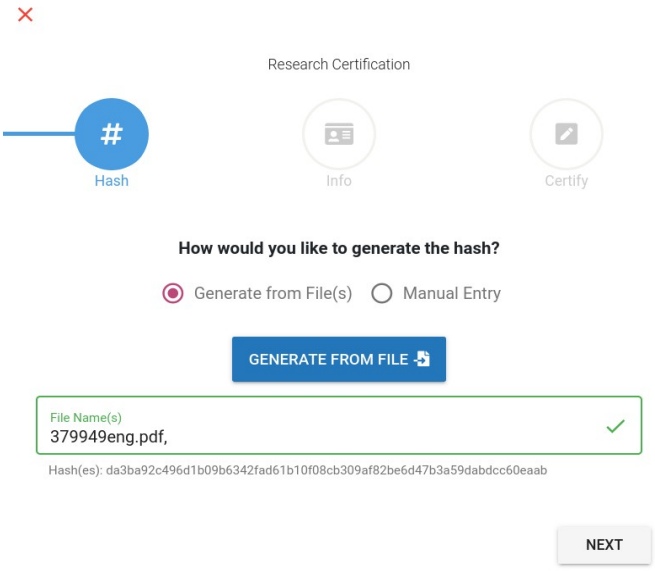


5. Bei erfolgter Attestierung werden dann die Informationen angezeigt, in welchem Block und zu welchem Datum der Existenznachweis vorliegt. Außerdem wird die endgültige Attestierungsdatei als Download ausgegeben, die den kompletten sequenziellen Ablauf des Hashings vom Dokument bis hin zur Verzeichnung auf der Blockchain enthält.
6. Über das Icon mit dem Informationszeichen können dann auch die kompletten Abläufe des Dokumentenhashings über die Calendar-Server bis zur Attestierung auf der Blockchain visuell nachvollzogen werden (aus Platzgründen hier nicht abgebildet).

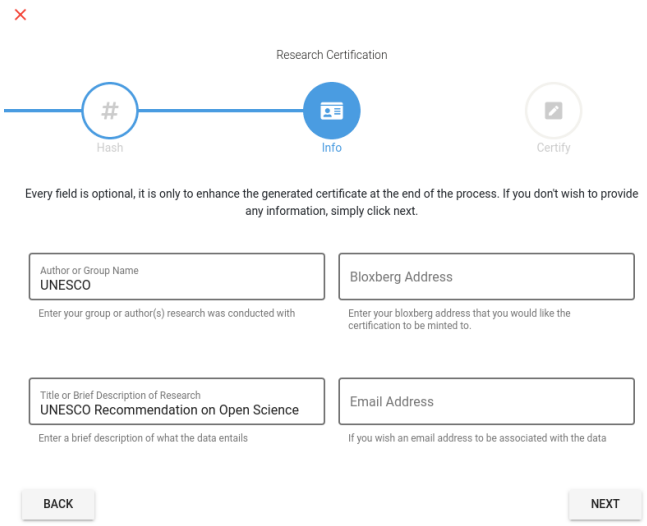
Anhang B: Attestierung des Beispieldokuments mit Bloxberg



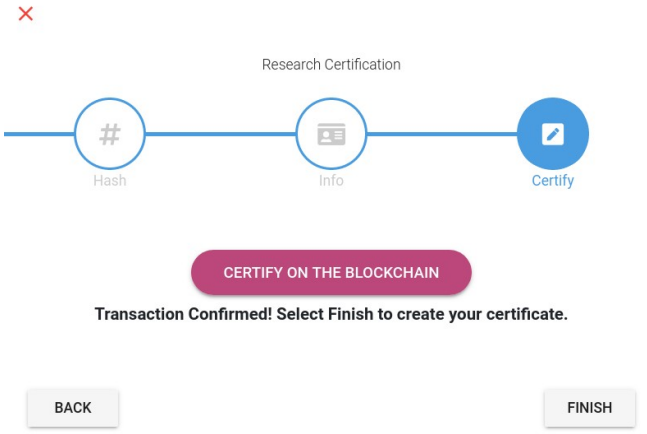
1. Die Erstellung des Existenznachweises erfolgt über die „Certify“-Sektion.



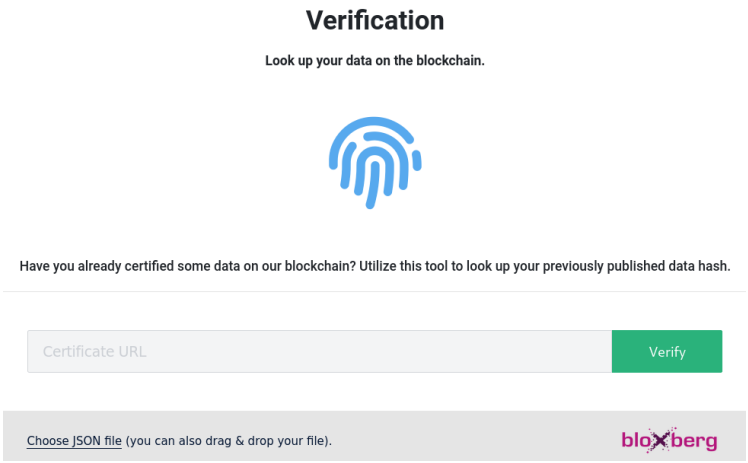
2. Zu Anfang wird das zu attestierende Dokument bzw. mehrere Dokumente ausgewählt (Generate from File) und daraus automatisch SHA256-Hashes erzeugt oder manuell ein Dokumentenhash eingefügt (Manual Entry).



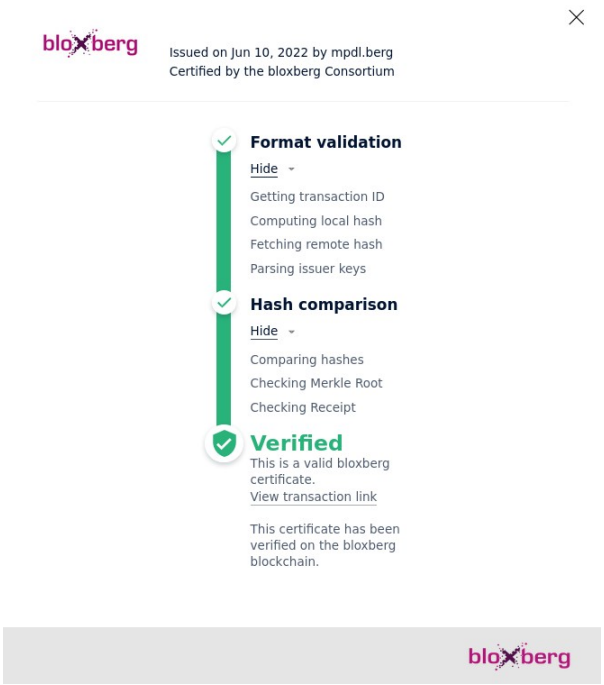
3. In einem weiteren Dialogfenster können optional Daten wie die Personen- oder Gruppennamen, Titel, eine spezifische Adresse auf der Bloxberg-Blockchain oder die E-Mail-Adresse angegeben werden.



4. Sobald der „Certify on the Blockchain“-Prozess mit einem Klick auf den Button angestoßen ist, erscheint nach kurzer Zeit eine Bestätigungsmeldung über die erfolgte Attestierung auf der Blockchain (Transaction Confirmed). Abschließend (mit einem Klick auf „Finish“) wird das PDF-Zertifikat in einem ZIP-Archiv als Download über den Browser ausgegeben.



5. Zur Verifizierung eines Existenznachweises wird die „Verify“-Sektion ausgewählt und dort das PDF-Zertifikat hochgeladen.



6. Im Anschluss öffnet sich ein Fenster, das dann die einzelnen Verifikationsschritte durchläuft und abschließend als Resultat den Status des Zertifikats ausgibt.

Anhang C: Daten CD-ROM / ZIP-Archiv

Zusätzliche Inhalte auf der beiliegenden CD-ROM bzw. im ZIP-Archiv:

`379949eng.pdf`

Attestiertes Beispieldokument (UNESCO Recommendation on Open Science)

SHA256: da3ba92c496d1b09b6342fad61b10f08cb309af82be6d47b3a59dabdcc60eaab

`2022-06-13-1531_379949eng.pdf.ots`

OpenTimestamps vorläufige Attestierungsdatei für das Beispieldokument

SHA256: 743ffaa2c587cc65f6018620ffa7b6c413ba82ef651ea2e0792bbe580a4f6db7

`2022-06-14-1915_379949eng.pdf.ots`

OpenTimestamps endgültige Attestierungsdatei für das Beispieldokument

SHA256: 9bb6b5247c6e5b3eb92b811366a2486f53de912d0b60af6a1029d756ba4286b7

`2022-06-10-1537_BloxbergDataCertificates.zip`

Bloxberg Research Certificate für das Beispieldokument

SHA256: dd0e6ad5cb10e268ac17bb5256f66749ca2352c86a25a00562895008049484ef

Quellenverzeichnis

Attah, E. (2020). *Five most prolific 51% attacks in crypto: Verge, Ethereum Classic, Bitcoin Gold, Feathercoin, Vertcoin*. CryptoSlate. https://cryptoslate.com/prolific-51-attacks-crypto-verge-ethereum-classic-bitcoin-gold-feathercoin-vertcoin/

Bach, N. (2021). Dezentrale Identifikatoren (DIDs): Die nächste PID-Evolution: Selbstsouverän, datenschutzfreundlich, dezentral. *o-bib. Das offene Bibliotheksjournal / Herausgeber VDB*, *8*(4), 1–20. https://doi.org/10.5282/O-BIB/5755

Bakos, Y., Halaburda, H., & Mueller-Bloch, C. (2021). When permissioned blockchains deliver more decentralization than permissionless. *Communications of the ACM*, *64*(2), 20–22. https://doi.org/10.1145/3442371

Bitcoin Wiki. (2014). *Proof of Publication*. https://en.bitcoin.it/w/index.php?title=Proof_of_Publication&oldid=48135

Bitcoin Wiki. (2015). *Proof of Ownership*. https://en.bitcoin.it/w/index.php?title=Proof_of_Ownership&oldid=59167

Bitcoin Wiki. (2017). *Principles of Bitcoin*. https://en.bitcoin.it/w/index.php?title=Principles_of_Bitcoin&oldid=63920

Bitcoin Wiki. (2018a). *Economic majority*. https://en.bitcoin.it/w/index.php?title=Economic_majority&oldid=64729

Bitcoin Wiki. (2018b). *New York Agreement*. https://en.bitcoin.it/w/index.php?title=New_York_Agreement&oldid=64781

Bitcoin Wiki. (2020). *Weaknesses*. https://en.bitcoin.it/w/index.php?title=Weaknesses&oldid=68022#Attacker_has_a_lot_of_computing_power

BitInfoCharts. (2022a). *Bitcoin Avg. Transaction Fee Chart*. https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

BitInfoCharts. (2022b). *Bitcoin Block Time Chart*. https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html

BitInfoCharts. (2022c). *Bitcoin (BTC) statistics—Price, Blocks Count, Difficulty, Hashrate, Value*. https://bitinfocharts.com/bitcoin/

Blockcerts. (2022). *Introduction*. Guide. https://www.blockcerts.org/guide/

Blockchain Bird. (2022). *Blockchain Misconceptions: Proof-of-stake coins are far more sustainable than mining bitcoin*. https://blockchainbird.org/t/bcb/card/proof-of-stake

Blockchain.com. (2009). *Block 0*. Bitcoin Explorer. https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Bloxberg Mainnet Explorer. (2019). *Block 1*. Block Details. https://blockexplorer.bloxberg.org/blocks/1/transactions

Bloxberg Mainnet Explorer. (2022). https://blockexplorer.bloxberg.org/

Bloxberg Validators DApp. (2022). https://validators.bloxberg.org/

Bloxberg.org. (2022). https://bloxberg.org/

Bundesamt für Sicherheit in der Informationstechnik. (2020). *Migration zu Post-Quanten-Kryptografie: Handlungsempfehlungen des BSI*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1

Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

Cambridge Centre for Alternative Finance. (2022). *Cambridge Bitcoin Electricity Consumption Index (CBECI)*. https://ccaf.io/cbeci/index

Coin Dance. (2022). *Bitcoin Nodes Summary*. https://coin.dance/nodes

CoinGecko. (2022a). *Bitcoin Price*. https://www.coingecko.com/en/coins/bitcoin

CoinGecko. (2022b). *Ethereum Price*. https://www.coingecko.com/en/coins/ethereum

DIN 31647:2015-05, Information und Dokumentation—Beweiswerterhaltung kryptographisch signierter Dokumente. (2015). Beuth Verlag. https://doi.org/10.31030/2294467

DIN/TS 31648:2021-04, Kriterien für vertrauenswürdige Transaktionen—Records Management und Beweiswerterhaltung in Distributed Ledger Technologien und Blockchain. (2021). Beuth Verlag. https://doi.org/10.31030/3211422

DomainTools. (2022). *Whois Record for bloxberg.org*. Whois Lookup. https://whois.domaintools.com/bloxberg.org

Ethereum.org. (2022a). *Ethereum Whitepaper*. https://ethereum.org/en/whitepaper/

Ethereum.org. (2022b). *The Merge*. https://ethereum.org/en/upgrades/merge/

Etherscan. (2015). *Block #0*. Ethereum (ETH) Blockchain Explorer. http://etherscan.io/block/0

Etherscan. (2022). *Ethereum Node Tracker*. http://etherscan.io/nodetracker

Fanta, A. (2022). *Interne Dokumente: EU tüftelt an Bitcoin-Verbot*. netzpolitik.org. https://netzpolitik.org/2022/interne-dokumente-eu-tueftelt-an-bitcoin-verbot/

Fill, H.-G., & Meier, A. (2020). *Blockchain kompakt: Grundlagen, Anwendungsoptionen und kritische Bewertung*. Springer Vieweg. https://doi.org/10.1007/978-3-658-27461-0

Gipp, B., Meuschke, N., & Gernandt, A. (2015). Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. *iConference 2015 Proceedings*. iConference 2015, Newport Beach, California. https://hdl.handle.net/2142/73770

GitHub. (2021). *BLIP 4*. Bloxberg Improvement Proposals. https://github.com/bloxberg-org/blips/blob/master/blips/blip-4-consensusupgrade.md

GitHub. (2022a). *Block explorer verification · Issue #127 · opentimestamps/opentimestamps-client*. Issues. https://github.com/opentimestamps/opentimestamps-client/issues/127

GitHub. (2022b). *Bloxberg*. Repositories. https://github.com/orgs/bloxberg-org/repositories

GitHub. (2022c). *How to „Add your company“ to the Member section of the website · Issue #2 · opentimestamps/opentimestamps.org*. Issues. https://github.com/opentimestamps/opentimestamps.org/issues/2

GitHub. (2022d). *OpenTimestamps*. People. https://github.com/orgs/opentimestamps/people

GitHub. (2022e). *Opentimestamps/opentimestamps-server*. Commits. https://github.com/opentimestamps/opentimestamps-server/commits/master?after=ac67218c3d45a93519bea0ec151b1e3629f87bd5+454&branch=master&qualified_name=refs%2Fheads%2Fmaster

GitHub. (2022f). *Opentimestamps-server*. REST API. https://api.github.com/repos/opentimestamps/opentimestamps-server

Guckelberger, A. (2019). Blockchain. In *Öffentliche Verwaltung im Zeitalter der Digitalisierung: Analysen und Strategien zur Verbesserung des E-Governments aus rechtlicher Sicht* (1. Auflage, S. 131–142). Nomos.

Haber, S., & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document. In A. J. Menezes & S. A. Vanstone (Hrsg.), *Advances in Cryptology-CRYPT0’ 90* (Bd. 537, S. 437–455). Springer. https://doi.org/10.1007/3-540-38424-3_32

Härer, F., & Fill, H.-G. (2020). *Blockchain-basierte Attestierung von Identitäten und Dokumenten*. https://doi.org/10.5281/ZENODO.3690139

Heller, L. (2019). *Wie Blockchain und Big Data Wissenschaftskommunikation, Informationsmärkte und digitale Teilhabe verändern*. AjBD Vortragsveranstaltung, Leipzig. https://nbn-resolving.org/urn:nbn:de:0290-opus4-162657

Hyla, T., & Pejaś, J. (2020). Long-term verification of signatures based on a blockchain. *Computers & Electrical Engineering*, *81*, 106523. https://doi.org/10.1016/j.compeleceng.2019.106523

Kemp, A. de. (2018). Blockchain for Science: Wissenskommunikation als offene Volkswirtschaft denken – und gestalten. *BIT online*, *21*(4), 332–337.

Kleinfercher, F., Vengadasalam, S., & Lawton, J. (2020). *Bloxberg: The Trusted Research Infrastructure: Whitepaper 1.1*. https://bloxberg.org/wp-content/uploads/2020/02/bloxberg_whitepaper_1.1.pdf

Kosmarski, A. (2020). Blockchain Adoption in Academia: Promises and Challenges. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(4), 117. https://doi.org/10.3390/joitmc6040117

Lawton, J. (2019). *On MPDL Bloxberg BFS initiative, status and outlook*. 2nd International Conference on Blockchain for Science, Research and Knowledge, Berlin. https://www.youtube.com/watch?v=-m0R8QdlhLI

Leible, S., Schlager, S., Schubotz, M., & Gipp, B. (2019). A Review on Blockchain Technology and Blockchain Projects Fostering Open Science. *Frontiers in Blockchain*, *2*, 16. https://doi.org/10.3389/fbloc.2019.00016

Manz, O. (2019). *Verschlüsseln, Signieren, Angreifen: Eine kompakte Einführung in die Kryptografie*. Springer Spektrum. https://doi.org/10.1007/978-3-662-59591-6

Mienert, H., Hepp, T., & Gipp, B. (2019). *Prioritätsnachweis des Urhebers durch blockchainbasierten Zeitstempel*. https://doi.org/10.5281/ZENODO.2547964

MPDL. (2022a). *Fourth bloxberg Summit 2022*. Pressemitteilungen. https://www.mpdl.mpg.de/ueber-uns/presse/812-fourth-bloxberg-summit-2022.html

MPDL. (2022b). *Organisation*. Über uns. https://www.mpdl.mpg.de/ueber-uns/organisation.html

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

OpenTimestamps.org. (2022). https://opentimestamps.org/

Oyelude, A. A. (2019). What's trending in blockchain technology and its potential uses in libraries. *Library Hi Tech News*, *36*(9), 17–18. https://doi.org/10.1108/LHTN-09-2019-0062

Pohlmann, N. (2019). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer Vieweg. https://doi.org/10.1007/978-3-658-25398-1

Prinz, W., Rose, T., Osterland, T., & Putschli, C. (2018). Blockchain: Verlässliche Transaktionen. In R. Neugebauer (Hrsg.), *Digitalisierung: Schlüsseltechnologien für Wirtschaft und Gesellschaft* (1. Auflage, S. 311–319). Springer Vieweg.

Raj, K. (2019). *Foundations of Blockchain: The pathway to crytocurrencies and decentralized blockchain applications*. Packt Publishing.

Ramamurthy, B. (2020). *Blockchain in Action*. Manning Publications.

Rizzo, P. (2021). *The Last Days of Satoshi: What Happened When Bitcoin's Creator Disappeared*. Bitcoin Magazine. https://bitcoinmagazine.com/technical/what-happened-when-bitcoin-creator-satoshi-nakamoto-disappeared

Schiller, K. (2022a). *Blockchain-as-a-Service (BaaS): Die Blockchain Dienstleister*. Blockchainwelt. https://blockchainwelt.de/blockchain-as-a-service-baas/

Schiller, K. (2022b). *Proof of Authority – Eine Alternative zum Proof of Stake?* Blockchainwelt. https://blockchainwelt.de/proof-of-authority-poa/

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). Ein Blick auf aktuelle Entwicklungen bei Blockchains und deren Auswirkungen auf den Energieverbrauch. *Informatik Spektrum*, *43*(6), 391–404. https://doi.org/10.1007/s00287-020-01321-z

Semar, W., & Beck, S. (2013). Sicherheit von Informationssystemen. In R. Kuhlen, W. Semar, & D. Strauch (Hrsg.), *Grundlagen der praktischen Information und Dokumentation* (S. 466–478). De Gruyter Saur. https://doi.org/10.1515/9783110258264.466

Shawn, L. W. M., Murali Mohan, P., Loh Kok Keong, P., & Balachandran, V. (2021). Blockchain-based Proof of Existence (PoE) Framework using Ethereum Smart Contracts. *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, 301–303. https://doi.org/10.1145/3422337.3450319

Streim, A., & Faupel, B. (2021). *Deutsche Wirtschaft kommt bei der Blockchain nicht voran*. Bitkom Pressemitteilung. https://www.bitkom.org/Presse/Presseinformation/Deutsche-Wirtschaft-kommt-bei-der-Blockchain-nicht-voran

Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (First Edition). O'Reilly.

Tante. (2022). *It's important but not the point*. https://tante.cc/2022/04/25/its-important-but-not-the-point/

Tasca, P., & Tessone, C. J. (2019). A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger*, *4*, 1–39. https://doi.org/10.5195/ledger.2019.140

Todd, P. (2016). *OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin*. https://petertodd.org/2016/opentimestamps-announcement

Todd, P. (2017a). *How OpenTimestamps „Carbon Dated" (almost) The Entire Internet With One Bitcoin Transaction*. https://petertodd.org/2017/carbon-dating-the-internet-archive-with-opentimestamps

Todd, P. (2017b). *Scalable Semi-Trustless Asset Transfer via Single-Use-Seals and Proof-of-Publication*. https://petertodd.org/2017/scalable-single-use-seal-asset-transfer

Todd, P. (2017c). *SHA1 Is Broken, But It's Still Good Enough for OpenTimestamps*. https://petertodd.org/2017/sha1-and-opentimestamps-proofs

Todd, P. (2018a). *[Ots-dev] GDPR and OTS calendars*. https://lists.opentimestamps.org/pipermail/ots-dev/2018-May/000052.html

Todd, P. (2018b). *[ots-dev] Proposal: Add https://*.calendar.catallaxy.com to default calendar whitelist*. https://lists.opentimestamps.org/pipermail/ots-dev/2018-March/000040.html

Todd, P. (2019). *[Ots-dev] Removing ETH/keccak support*. https://lists.opentimestamps.org/pipermail/ots-dev/2019-August/000091.html

UNESCO. (2021). *UNESCO Recommendation on Open Science*. https://unesdoc.unesco.org/ark:/48223/pf0000379949

Universität Konstanz. (2022). *Glossar: Prüfsumme*. forschungsdaten.info. https://www.-forschungsdaten.info/praxis-kompakt/glossar/#c500907

Wayner, P. (1997). *British Document Outlines Early Encryption Discovery*. The New York Times. https://archive.nytimes.com/www.nytimes.com/library/cyber/week/122497encrypt.html

Weilbach, W. T. (2017). *Practical Application of Distributed Ledger Technology in Support of Digital Evidence Integrity Verification Processes*. https://hdl.handle.net/10962/61872

Wittek, K., Krakau, D., Wittek, N., Lawton, J., & Pohlmann, N. (2020). Integrating bloxberg's Proof of Existence Service With MATLAB. *Frontiers in Blockchain*, *3*, 546264. https://doi.org/10.3389/fbloc.2020.546264

Wittek, K., Wittek, N., Lawton, J., Dohndorf, I., Weinert, A., & Ionita, A. (2021). *A Blockchain-Based Approach to Provenance and Reproducibility in Research Workflows*. 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia. https://doi.org/10.1109/ICBC51069.2021.9461139

Woodard, J. (2021). Using IPFS, Filecoin and the Wolfram Language to Build a Unified Decentralized Services Interface. *Wolfram Blog*. https://blog.wolfram.com/2021/05/12/using-ipfs-filecoin-and-the-wolfram-language-to-build-a-unified-decentralized-services-interface/

Wüst, K., & Gervais, A. (2018). Do you need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45–54. https://doi.org/10.1109/CVCBT.2018.00011