ZfdG

Zeitschrift für digitale Geisteswissenschaften

Artikel aus:
Zeitschrift für digitale Geisteswissenschaften

Titel:
Blockchain für die Geisteswissenschaften? Möglichkeiten des Einsatzes von Blockchain und verwandten Technologien für wissenschaftliche Publikationen

Autor/in:
Anna Neovesky

Kontakt: anna.neovesky@adwmainz.de
Institution: Akademie der Wissenschaften und der Literatur, Mainz
GND: 1185804625 ORCID: 0000-0002-0627-8199

Autor/in:
Julius Peinelt

Kontakt: julius.peinelt@futurice.com
Institution: Futurice GmbH
GND: 1185806768 ORCID: 0000-0001-8842-0728

DOI des Artikels:
10.17175/2019_003

Nachweis im OPAC der Herzog August Bibliothek:
1016003919

Erstveröffentlichung:
03.07.2019

Letzte Überprüfung aller Verweise:
22.05.2019

GND-Verschlagwortung:
Blockchain | Forschungsdaten | elektronisches Publizieren | Technologietransfer | Transaktionssystem |

Zitierweise:
Anna Neovesky, Julius Peinelt: Blockchain für die Geisteswissenschaften? Möglichkeiten des Einsatzes von Blockchain und verwandten Technologien für wissenschaftliche Publikationen. In: Zeitschrift für digitale Geisteswissenschaften. Wolfenbüttel 2019. PDF Format ohne Paginierung. Als text/html abrufbar unter DOI: 10.17175/2019_003.

Anna Neovesky, Julius Peinelt

Blockchain für die Geisteswissenschaften? Möglichkeiten des Einsatzes von Blockchain und verwandten Technologien für wissenschaftliche Publikationen

Abstracts

Spätestens nach dem Kurshoch von Bitcoin Ende 2017 ist Blockchain den meisten ein Begriff und auch in der Wissenschaft werden aktuell Einsatzmöglichkeiten diskutiert und erprobt. Insbesondere die Transparenz, Nachvollziehbarkeit und Unveränderlichkeit der in einer Blockchain gespeicherten Inhalte sowie die Dezentralität des Systems sind von besonderem Interesse. Als Einsatzbereiche, die auch für die Geisteswissenschaften interessant sind, werden vor allem die wissenschaftliche Publikation von Artikeln und Forschungsdaten sowie blockchain-basierte Möglichkeiten der Signierung von publizierten Inhalten diskutiert. Anhand des konkreten Beispiels einer wissenschaftlichen Zeitschrift wird im Folgenden die Funktionsweise von Blockchain erläutert und Einsatzmöglichkeiten sowie Vorbehalte dargestellt und diskutiert.

The term blockchain is well known to many, at least since the high of Bitcoin prices at the end of 2017. Its application potentials are discussed and tested in economy and science. Especially the transparency, traceability and unchangeability of the content stored in a blockchain and the decentralization are of particular interest. Potential areas of application that are also of interest for the humanities are discussed in this paper, especially the scientific publication of articles and research data as well as blockchain-based possibilities for signing published content. Based on the concrete example of a scientific journal, the functionality, potential application and caveats of blockchain will be explained and discussed.

1. Blockchain und Geisteswissenschaften?

Blockchain sowie Bitcoin, die auf der Blockchain-Technologie basierende Kryptowährung, waren mit Sicherheit die meistdiskutierte Technologie 2017. Von der begeisterten Ausrufung einer »Revolution« bis hin zu kritischeren Tönen wurde eine weite Spanne von Positionen diskutiert. In der Tendenz wurde die neue Technologie jedoch begeistert aufgenommen.[1] Auch wenn der Bitcoin-Kurs seitdem kontinuierlich gesunken ist, bleibt die dahinterstehende Blockchain-Technologie nach wie vor ein weitdiskutiertes Thema.[2]

Der populärste Anwendungsbereich für Blockchain sind Kryptowährungen. Die Idee dahinter ist das Schaffen einer Währung, die manipulationssicher und unabhängig von kontrollierenden Eingriffen von Seiten der Regierungen und Banken ist. Diese Unabhängigkeit wird dadurch gewährleistet, dass die Transaktionen offen in einem dezentralen System durchgeführt werden und somit nicht die Kontrolle einer zentralen Instanz ermöglichen und brauchen.

Erste Versuche und schließlich auch Bitcoin kamen aus dem Umfeld der Cypherpunk Mailingliste,[3] in der vor allem libertäre marktwirtschaftliche Ansätze sowie der Schutz der Privatsphäre durch Kryptographie diskutiert wurden. Inzwischen wird versucht, Blockchain-Technologien auch in anderen Bereichen wie der Logistik, dem Gesundheitswesen sowie für das Internet der Dinge einzusetzen. Ein zentrales Thema ist hierbei immer die Möglichkeit, den verarbeiteten Daten trauen zu können, ohne eine zentrale Instanz zur Datenerzeugung, -bereitstellung oder -kuratierung zu benötigen. Es gibt auch Beispiele für dezentrale Formen etablierter Plattformen, wie zum Beispiel die Blockchain-basierte Social Media Plattform Steemit.

Auch in der Forschungslandschaft wird diskutiert, welche Innovationen und welche Verbesserungen Blockchain der Wissenschaft bieten kann. Neueingerichtete Forschungszentren und Think Tanks, [4] darunter das Blockchain-Labor des Fraunhofer-Instituts für Angewandte Informationstechnik und Forschungscluster an Universitäten,[5] evaluieren die Einsatzmöglichkeiten von Blockchain.[6] Es gibt bereits erste Anwendungen, die im Rahmen von Forschungsprojekten, teils in Kooperation mit der freien Wirtschaft, veröffentlicht wurden.[7] Der Fokus bei den Anwendungen und Forschungsbereichen liegt auf der Kryptoökonomie sowie auf Themen der Industrie 4.0, vor allem auf automatischen Fertigungstechniken sowie im Gesundheitswesen. Auch in die universitäre Lehre hat Blockchain Eingang gefunden.[8] So wird seit 2018 an der Hochschule Mittweida im Bereich Informatik der Master-Studiengang Blockchain & Distributed Ledger Technologies (DLT) angeboten. Anfang November 2018 fand in Berlin die erste »Blockchain for Science Conference« statt, in der es besonders um Anwendungen im Bereich Open Science, wissenschaftlichem Publizieren und Forschungsdaten ging.

[1] »Blockchain soll 2018 das Internet der Dinge revolutionieren«, vgl. Kern 2017 sowie Blockchain als »die nächste Evolutionsstufe des Internets«, vgl. Lenz 2017.
[2] Von Eichhorn 2018, S. 71.
[3] Wikipedia: Cypherpunk.
[4] Für einen Überblick über Forschungszentren in Europa vgl. Süssenguth / Liebenstund 2018, S. 48.
[5] So das Center for Distributed Ledgers and Contracts der TU Darmstadt, das Blockchain Research Cluster der TU München und das Blockchain Competence Center der HS Mittweida.
[6] Zu den Ergebnissen vgl. die Positionspapiere Grech / Camilleri 2017, passim; Meinel et al. 2018, passim und Schlatt et al. 2016, passim.
[7] Für einen Überblick über Ideen, Anwendungen und Tools in der Wissenschaft vgl. das kollaborative Dokument Bartling 2017, S. 12–23.
[8] Für einen Überblick über internationale Studienangebote zur Blockchain-Technologie vgl. Brien 2017, passim.

Für Blockchain-Anwendungen in der Wissenschaft, die auch in Bezug auf die Geisteswissenschaften besonders relevant sind, werden insbesondere folgende Bereiche diskutiert: Open Access-Publikationen, Sicherstellung der Reproduzierbarkeit von Forschungsdaten, Verwaltung und Versionierung von Forschungsdaten, wissenschaftliche Kommunikation, Peer-Review-Verfahren, Verteilung von Fördermitteln, Vergabe von Credits für wissenschaftliche Leistungen sowie als Prüfsystem für Zertifikate in MOOCs (Massive Open Online Courses).[9] Auch für den Bereich der Archivierung und der nachhaltigen Sicherung von Forschungsdaten könnte Blockchain zusätzlich zu zentralen Einrichtungen eine dezentrale, von der Community getragene Ergänzung sein.

Dieser Beitrag[10] gibt zunächst eine Einführung in Konzept und Funktionsweise von Blockchain und diskutiert diese dann anhand des Beispiels des wissenschaftlichen Publizierens. Hierbei werden sowohl Bereiche diskutiert, die mittels Blockchain implementiert werden können, als auch technologische und konzeptionelle Fragen. Es folgt ein Überblick über weitere Blockchain-verwandte Technologien. So werden die theoretischen Überlegungen für den Einsatz von Blockchain anhand eines konkreten Beispiels illustriert und die Anwendbarkeit diskutiert sowie technologische und konzeptionelle Fragen aufgezeigt.

2. Funktionsweise von Blockchain

2.1 Was ist Blockchain?

Eine Blockchain ist grundsätzlich eine Liste von Datensätzen. Diese Datensätze werden Blöcke genannt und die Liste dieser Datensätze folglich Blockkette – Blockchain. Der Begriff ist außerdem der Name für ein Konzept: ein dezentrales System der Buchführung von grundsätzlich jeder Art von Inhalt. Blockchain ist die technische Basis für Kryptowährungen, aber auch für andere Anwendungen. Das Neue an Blockchain ist eine verteilte Konsensfindung, die keine zentrale Instanz benötigt, sondern rein Peer-to-Peer funktioniert. Damit sind die direkte Kommunikation, die Unabhängigkeit von zentralen Institutionen, Transparenz und die Unveränderlichkeit der in der Blockchain gespeicherten Inhalte jene Aspekte, die als besondere Vorteile gegenüber anderen Verfahren gesehen werden.[11]

2.2 Wie funktioniert Blockchain?

Für einen Überblick über die Funktionsweise von Blockchain[12] wird zunächst die Implementierung der bekanntesten Blockchain, das Bitcoin-Protokoll, vorgestellt: Bitcoin ist die älteste existierende Blockchain (seit Januar 2009)[13] und die erste dezentralisierte digitale Währung. Früher wurden beide Begriffe oft synonym genutzt, nach einer ersten geplatzten Bitcoin-Blase und dem Entstehen weiterer auf der Blockchain basierenden Währungen und Technologien folgte jedoch eine stärkere Differenzierung bei der Benennung.

Die Blockchain setzt sich aus Blöcken zusammen, die jeweils aus einem Header und den Transaktionsdaten bestehen. Der Header enthält:[14]

- Einen Hashpointer auf den vorherigen Block. Dieser kryptographische Schlüssel stellt die Unveränderbarkeit des vorherigen Elements sicher.
- Eine Nonce. Dieser 32-bit Wert besteht aus einer Zeichenkette und wird temporär als Identifikator eingesetzt. Dies spielt bei der Erstellung neuer Transaktionen eine Rolle.
- Den Root Node, den Wurzelknoten des Transaktionsbaumes, also den ersten Eintrag in einer Kette. Durch diesen ist belegt, dass die Daten in den Baumblättern unverändert sind.
- Einen Zeitstempel, der das Datum der Transaktion angibt.

[9] Zu verschiedenen Einsatzmöglichkeiten von Blockchain im Wissenschaftlichen Kontext vgl. Chen et al. 2018; Grech / Camilleri 2017, S. 51–76; Fecher / Bartling 2016, passim; sowie van Rossum 2017, S. 7–12.
[10] Die Autorin und der Autor möchten Jana Hänßler, Timo Kissinger, Gabriel Reimers und Patrick Toschka für wertvolle Anregungen bei der Vorbereitung und Redaktion des Manuskripts danken. Ein besonderer Dank gilt dem Spice Program der Futurice GmbH.
[11] Vgl dazu u.a. Gerch / Camilleri 2017 , S. 8 und S. 18–22.
[12] Für eine visuelle Blockchain-Demo vgl. Brownworth 2017. Als Beispiel für eine minimale Blockchain-Implementierung mit JavaScript vgl. Tillmann 2018.
[13] Nakamoto 2008.
[14] Narayanan et al. 2016, S. 64–65.

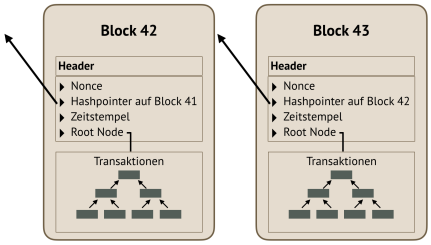

Abb. 1: Block bestehend aus Header und Transaktionsdaten. [Anna Neovesky / Julius Peinelt 2018. CC BY 4.0.]

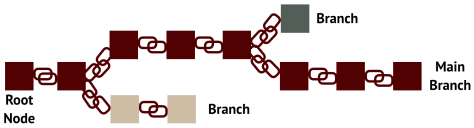

Abb. 2: Blöcke in der Blockchain mit dem aktuellen Branch, dem Main Branch und nicht mehr weiterverfolgten Branches (beige und grau). [Anna Neovesky / Julius Peinelt 2018. CC BY 4.0.]

Die Transaktionsdaten sind die Änderungen, die der Blockchain hinzugefügt werden sollen, zum Beispiel der Transfer eines Bitcoins auf ein anderes Konto oder eine Änderung an den in einer Blockchain gespeicherten Daten. Transaktionsdaten werden in einem Merkle tree gespeichert. Ein Merkle tree,[15] auch Hash tree genannt, ist eine Datenstruktur, die Daten in einer Baumstruktur ablegt. Sie spielt in der Kryptografie eine große Rolle, findet aber ebenso beim Quellcode-Verwaltungs-Tool Git Anwendung. Das wesentliche Charakteristikum besteht darin, dass die Struktur des Merkle trees ermöglicht, Daten auf ihre Integrität zu prüfen, ohne über den gesamten Datenbestand zu verfügen.

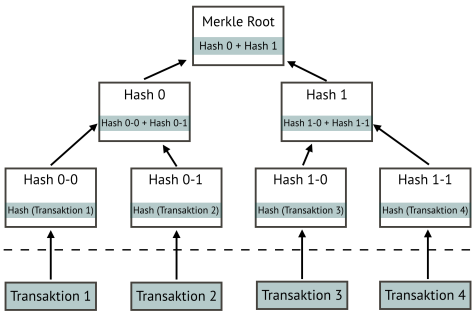

Abb. 3: Schema eines Merkle tree. [Anna Neovesky / Julius Peinelt 2018, aufbauend auf Hash Tree von Becky In: bitcoinwiki 2018. CC BY 4.0.]

Um eine neue Transaktion auszuführen, muss ein neuer Block erstellt und an die Blockchain angehängt werden. Hierbei spielen der Merkle tree und die Hashfunktion des Systems sowie die Nonce eine Rolle.

Eine Hashfunktion ist eine Funktion, die aus einem Inhalt eine kürzere Zeichenkette, den Hashwert, errechnet. Der Hashwert dient als Prüfsumme für den Inhalt. Eine Veränderung des Inhalts führt immer auch zu einer Änderung des Hashwerts. Manipulationen können so leicht erkannt werden. Bei Bitcoin kommt die kryptographische Hashfunktion SHA-256 zum Einsatz.[16]

Um eine Transaktion durchzuführen, werden zuerst Transaktionen aus einem netzwerkweiten Transaktionspool ausgewählt. Dieser Pool enthält alle noch nicht ausgeführten Transaktionen und kann als eine Art Warteliste verstanden werden, denn durch die im Bitcoin-Protokoll festgelegte Blockgröße ist die Anzahl der Transaktionen pro Sekunde limitiert, die in einem Block bearbeitet werden können. Aus den ausgewählten Transaktionen wird zunächst ein Merkle tree erstellt. Daraufhin wird mittels Hashfunktion ein Hashwert aus dem Header des Blocks, der den Root node des Merkle trees enthält, errechnet. Die Nonce wird hierbei genutzt, um einen gültigen Block zu finden, dessen Hashwert einen festgelegten Grenzwert nicht überschreiten darf. Dazu wird die Nonce im neuen Blockheader zufällig verändert, da der errechnete Hashwert nicht vorhersehbar ist. Das wiederholte Ändern der Nonce und die Neuberechnung des Hashes wird Mining genannt und ist sehr rechenintensiv.[17]

[15] Merkle 1988, passim.
[16] Vgl. Wikipedia: SHA-2.
[17] Narayanan et al. 2016, S.105–107.

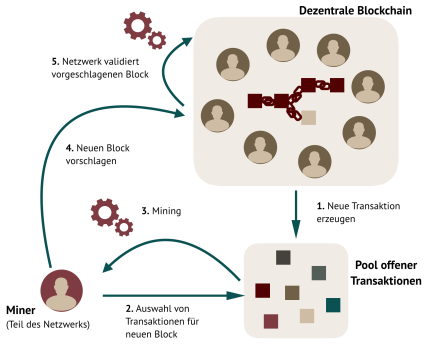

Abb. 4: Vereinfachte Darstellung des Ablaufs einer Transaktion. [Anna Neovesky / Julius Peinelt 2018. CC BY 4.0.]

Wird ein Wert für die Nonce gefunden, mit dem der Hash unter dem Grenzwert liegt, wird der Block im Netzwerk vorgeschlagen. Wenn dieser vom Netzwerk akzeptiert wird, erhält die ausführende Partei, die den Block gefunden hat, der Node , eine Belohnung in Form von Bitcoins. Ein Node in einem Blockchain-Netzwerk ist jeder Computer, der das Bitcoin-Protokoll, also den Programmcode von Bitcoin, ausführt. Der Node ist damit Teilnehmer im Netzwerk. Da die Validität eines Blocks durch die rechenintensive Erzeugung eines Hashwertes erreicht wurde, nennt man diesen Vorgang Proof-of-Work. Der Grenzwert wird im Bitcoin-Netzwerk periodisch der Rechenleistung des gesamten Netzwerks angepasst, um eine gleichbleibende Rate an neu geschaffenen Blöcken sicherzustellen, so dass eine eventuelle Synchronisation des Netzwerks sichergestellt werden kann. Es existieren auch andere Konsensfindungsverfahren wie Proof-of-Stake , das zum Beispiel bei Peercoin[18] Anwendung findet, bei dem Teilnehmer*innen mit einem Teil ihrer Tokens, also Einheiten der blockchainspezifischen Währung, darüber abstimmen können, welcher Block als neuer valider Block an die Blockchain angehängt wird.

Ist ein Konsens gefunden, arbeiten alle Nodes im Netzwerk nun mit diesem Block, an den sie weitere Blöcke anhängen können, wodurch die Kette verlängert wird.

Da man in einem verteilten Netzwerk auch immer mit Latenzen rechnen muss, kann es durchaus vorkommen, dass mehrere Teilnehmer*innen – mehr oder weniger gleichzeitig – einen neuen gültigen Block finden. In einem solchen Fall arbeiten verschiedene Teile des Netzwerks mit jeweils einem der gefundenen Blöcke weiter und erstellen sogenannte Branches. Der rechenstärkste Teil wird nach einigen weiteren gefundenen Blöcken einen längeren Branch als die anderen Teilnehmer*innen erzeugen. Da der längste Branch als der für alle Teilnehmer*innen gültige angesehen wird, gehen auch alle anderen dazu über, an diesem weiter zu arbeiten, Transaktionen in kürzeren Branches werden wieder dem Transaktionspool als unbearbeitet zugeführt. Dieses Verhalten führt dazu, dass das Netzwerk insgesamt synchronisiert und aktualisiert bleibt.

Bei Bitcoin ist es daher erstrebenswert, möglichst schnell und – als Vorbedingung dazu – mit hoher Rechenleistung neue Blöcke zu erstellen. Dies führt zu einem erheblichen Energiebedarf für den Miningprozess. So lag der geschätzte[19] Stromverbrauch der Bitcoin Blockchain auf ihrem Höhepunkt 2018 bei ca. 73 TWh pro Jahr,[20] was ungefähr dem Verbrauch von Österreich entspricht. Es ist daher besonders attraktiv, Mining in Ländern mit niedrigen Strompreisen zu betreiben. Die größten Miningfarmen wurden in China und Hongkong eingerichtet und haben aktuell insgesamt fast die Hälfte der gesamten Miningpower des Bitcoinnetzwerkes.[21] Es liegen auch Berichte vor,[22] wonach unter diesen großen Minern Absprachen getroffen werden, was die Dezentralität der Blockchain gefährdet.

Für die Manipulationssicherheit einer Blockchain sorgt der Hashwert. In jedem Block ist der Hash des vorherigen Blocks enthalten. Dies verhindert, dass man nachträglich den Inhalt eines älteren Blocks der Blockchain ändern kann. Denn man müsste dann auch die Hashwerte aller nachfolgenden Blöcke neu berechnen. Eine Änderung des Blockinhalts verändert nämlich auch dessen Hashwert. Da der Hashwert eines Blocks einer der Parameter für den Hashwert des nachfolgenden Blocks ist, würde sich auch der Hashwert des nachfolgenden Blocks ändern. Unterlässt man die Neuberechnung und schlägt dem Netzwerk geänderte Blöcke vor, würde die Inkonsistenz der Hashwerte dem Netzwerk bei der Validierung der Blockchain auffallen und die Änderungen würden abgelehnt werden.

Der Hashwert bietet also zwei Vorzüge: Zum einen wäre die Neuberechnung der Hashwerte sehr rechenintensiv und müsste zudem noch schneller erfolgen als neue Blöcke an die Blockchain angehängt werden, zum anderen ist eine Datensparsamkeit gegeben, denn es müssen nicht immer alle Daten an alle Teilnehmer*innen übertragen werden oder von diesen gespeichert werden, die Kenntnis der Hashwerte alleine macht die Validität der Blockchain schon überprüfbar. Dadurch, dass alle Teilnehmer*innen Zugriff auf die Blockchain haben, kann jeder die Validität sicherstellen, womit die Dezentralität des Systems erreicht wird.

[18] King / Nadal 2012, passim.
[19] Die Schätzung basiert unter anderem auf einer Hochrechnung zu aktiven Minern und Kosten für die Kühlung der Maschinen. Vgl. Bitcoin Energy Consumption Index.
[20] Bitcoin Energy Consumption Index.
[21] Bitcoin Mining Pools und Bitcoin Mining in China zur Aufschlüsselung der Mining-Pools.
[22] Nakamura / Chen 2017, passim.

2.3 Verwandte Technologien: Private chains, Permissioned chains, Ledger, Distributed ledger und Smart contracts

Neben der bisher geschilderten offenen Blockchain gibt es auch Private chains und Permissioned chains. Beide sind Blockchains, bei denen die Teilnahme eingeschränkt ist. Hierbei stimmt das Netzwerk darüber ab,[23] ob ein neuer Node Teil des Netzwerks werden darf. Bei Private chains ist zudem die Blockchain insgesamt nicht öffentlich. Das heißt, nur die Teilnehmer*innen können sie einsehen, während bei der offenen Blockchain auch Nicht-Teilnehmende alle Daten sehen können.

Blockchain selbst baut auf bereits zuvor existierenden Konzepten auf und ist ein spezieller Typ eines distributed ledger. Ein Ledger[24] (dt. Kassenbuch) ist zunächst eine Software für kommandozeilenbasierte Buchführung. Die dezentrale, vernetzte Form einer solchen Transaktionsdatenbank ist der distributed ledger. Begrifflich werden distributed ledger oft nicht von der Blockchain abgegrenzt,[25] verfügen jedoch über einige andere Merkmale. Sie verzichten darauf, Transaktionen in Blöcken zusammenzufassen, das heißt, es findet kein Mining statt. Die Transaktionen werden stattdessen unmittelbar aneinandergehängt. Das bedeutet, dass Distributed Ledger weniger rechenintensiv sind als Blockchains mit Proof-of-Work-Verfahren. Die Konsensfindung findet bei Distributed Ledgers entweder manuell durch Bestätigung der Vertragspartner oder durch einen Notarservice statt.[26]

Ein Problem, das entsteht, wenn Transaktionen nicht blockweise verarbeitet werden, ist die Synchronisation im Netzwerk. Viele Distributed ledger sind daher so implementiert, dass nicht alle Transaktionsdaten allen im Netzwerk bekannt sind. Stattdessen besteht das öffentliche Netzwerk aus vielen kleineren privaten Netzwerken und Daten werden nur unter Parteien ausgetauscht, die auch Interesse und entsprechende Rechte an diesen Daten haben.[27] Vorteile dieser Herangehensweise sind der Verzicht auf teure Proof-of-Work-Berechnungen und die Möglichkeit, gewisse Daten privat zu halten. Dafür ist das System jedoch nicht offen und trustless, was die wesentlichen Motivationen für Blockchain sind.

Produkte wie Corda[28] bieten die Möglichkeit, die Konsensfindung im Netzwerk zwischen einzelnen Parteien individuell anzupassen und etwa auch auf vertrauenswürdige Drittparteien zurückzugreifen.

Ferner spielen in der Diskussion um den Einsatz von Blockchain im wissenschaftlichen Kontext Smart Contracts, ein Feature der ledger-Technologie, eine Rolle. Smart Contracts sind Computerprotokolle, die Verträge abbilden und in der Blockchain abwickeln und sind damit ein Teil des Blockchain-Protokolls.

Ein Smart Contract ist, technisch betrachtet, Code, der immer ausgeführt wird, wenn Nutzer*innen eine Nachricht als Teil einer Transaktion an ihn schicken. Miner führen den Code aus und erhalten dafür anfallende Gebühren. Ist ein Smart Contract dann Teil einer Blockchain, kann er nicht mehr verändert werden. Dies hat in der Vergangenheit immer wieder dazu geführt, dass bei der Entwicklung übersehene Fehler ausgenutzt wurden und Nutzer*innen dieser Smart Contracts hohe Verluste erlitten.[29]

	Public Blockchain	**Permissioned Blockchain**	**Private Ledger**
Zugriffsrechte	Frei für jeden zugänglich	Öffentlich einsehbar, aktive Teilnahme nur, wenn bestimmte Kriterien erfüllt werden	Zugriff und Teilnahme nur für zugelassene Parteien
Transaktionsrate	Langsam	Schnell	Schnell
Anonymität der Validatoren	Hoch	Niedrig	Niedrig
Konsensverfahren	Vor allem Proof of Work, Proof of Stake	Proof of Stake, Byzantinischer-Fehler-Toleranzverfahren[30]	Multisignaturen,[31] Byzantinischer-Fehler-Toleranzverfahren
Tokens (Gibt es eine »Währung«?)	Vorhanden und nötig	Vorhanden, nicht zwingend	Keine Tokens
Vertrauen in Teilnehmer*innen	Niedrig, »trustless«	Hoch	Hoch

Tab. 1: Tabelle zu Unterschieden und Gemeinsamkeiten von Public und Permissioned Blockchain sowie Private Ledger. [Anna Neovesky / Julius Peinelt 2018. CC BY 4.0.]

[23] Wie genau dies erfolgt, legt die Spezifikation des Protokolls zugrunde.
[24] vgl. Wiegley 2004 sowie Ledger.
[25] Für eine kurze Abgrenzung zwischen den Konzepten vgl. Slootweg 2016.
[26] Corda: Consensus.
[27] Hearn 2016, S. 12.
[28] Corda.
[29] Wikipedia: The DAO (organization).
[30] Bei diesem Verfahren wird von Beginn an davon ausgegangen, dass eine gewisse Anzahl an Akteur*innen bösartig argieren.
[31] Mehrere Personen müssen dem Verfahren zustimmen.

3. Blockchain Technologie an einem Beispiel aus der geisteswissenschaftlichen Praxis: Die Publikation wissenschaftlicher Artikel

3.1 Wieso Blockchain für wissenschaftliche Publikationen nutzen?

Einer der Anwendungsfälle, die besonders intensiv diskutiert werden, ist der Einsatz von Blockchain im Bereich der Publikation von wissenschaftlichen Artikeln.[32] Es gibt drei Hauptgründe hierfür: die Zunahme von Inhalten, die Open Access bereitgestellt werden, die Angst vor Plagiaten und die Frage der Qualitätssicherung.[33]

Auch eine Kritik an der marktbeherrschenden Position einiger weniger privatwirtschaftlicher Verlage, den teils hohen Kosten, die auf Autor*innen zukommen, die ihre Publikationen Open Access bereitstellen wollen und die langen Begutachtungsdauern führen zu dem Wunsch nach einer Unabhängigkeit von diesen zentralen Instanzen[34] und einem Demokratisierungsprozess im Bereich des wissenschaftlichen Publizierens.[35]

Der Einsatz von Blockchain als dezentralem Netzwerk wird auch für wissenschaftliche Publikationen diskutiert. Insbesondere die Transparenz und Sicherheit, die Blockchain bietet, spielen eine Rolle sowie der Wunsch, Flaschenhälse aufzulösen, die durch zentrale Strukturen entstehen.[36]

3.2. Der wissenschaftliche Publikationsprozess mit Blockchain

Wie könnte die Realisierung einer wissenschaftlichen Zeitschrift mit Blockchain aussehen? Hierzu stellt sich zunächst die Frage, aus welchen Schritten ein Publikationsprozess besteht und wie die entsprechenden Schritte mittels Blockchain-Technologie abgebildet werden könnten.

Als Schritte, die bei der Publikation in einem Open Access Journal zur Anwendung kommen, werden die Publikationsrichtlinien des vorliegenden eJournals herangezogen. Diese sind, wenn man eine Publikation mit anschließendem open peer-Reviewverfahren anstrebt:[37]

- Vorschlag einreichen
- Diskussion der Fachredaktion
- Feedback an Autor*innen
- Beitrag einreichen
- Redaktionelle Prüfung
- Veröffentlichung
- Autor*innen können Gutachter*innen vorschlagen
- Zweifach positiv evaluierte Artikel kommen in das jeweilige Jahrgangsheft

Zunächst gilt es zu klären, welche Technologie konkret eingesetzt werden soll, sowie welche Komponenten nachgenutzt werden können. Hierbei bieten sich zwei verschiedene Szenarien an: man kann ein bestehendes System nutzen, also beispielsweise auf der offenen Blockchain Ethereum aufbauen, oder eine eigene Blockchain beziehungsweise einen eigenen Ledger implementieren.

Wenn man ein bestehendes System wie Ethereum nutzt, ist man Teil eines offenen Netzwerks. Dieses übernimmt das Mining und man ist von dem Netzwerk abhängig. Wenn alle Teilnehmer*innen aus dem Netzwerk aussteigen, ist die Blockchain aufgrund fehlender Rechenleistung angreifbar (vgl. Kapitel 3.3). Dafür ist die Implementierung sehr einfach.

Nimmt man einen Distributed Ledger, stellt sich die Frage nach dem Konsensmodell, das man nutzen will und anderen Konfigurationen, wie der Offenheit des Netzwerkes. Es ist also Vorarbeit nötig. Bei permissioned chains befindet man sich innerhalb eines geschlossenen Netzwerks, man kann Parteien einladen, die Mehrheit der aktuellen Teilnehmer*innen des Netzwerks kann die Aufnahme genehmigen. Damit kann man sicherstellen, alle Parteien im Netzwerk zu kennen.

Nach dem Grad der Offenheit ist also die zweite Frage, die man sich stellen muss, die, ob man tatsächlich eine Blockchain mit Mining und Belohnungssystem braucht oder ein distributed ledger mit einem initial bestimmten Personenkreis zielführender ist. Nicht unbeachtet sollte dabei auch der schon angesprochene hohe Energiebedarf des Minings bleiben. Auch ist zu klären, ob der Prozess von Beginn an offen sein soll, oder erst ab einem bestimmten Zeitpunkt, wie etwa der Publikation des Manuskripts.

Unabhängig davon, für welche Blockchain-Technologie man sich entscheidet, ist in jedem Fall die Entwicklung einer Software nötig, die die auf der Blockchain aufbauende Anwendung implementiert. Die Software muss also für diesen Anwendungsfall unter anderem ein Public-Key-Verschlüsselungsverfahren unterstützen, mit dem alle Teilnehmer identifizierbar sind und Inhalte

[32] Vgl. dazu Taudes 2017.
[33] Fund 2017.
[34] Taudes 2017.
[35] Fund 2017.
[36] vgl. Heller 2017a.
[37] Zfdg: P wie Publizieren.

signieren können sowie eine Eingabemaske für die Inhalte bereitstellen und den Einreichungsprozess abbilden. Für einzelne Features können vorhandene Frameworks und Libraries nachgenutzt werden.[38]

Wie würde der Publikationsprozess exemplarisch ablaufen? Alle, die zu den Inhalten beitragen wollen – Autor*innen wie Gutachter*innen – müssen zunächst dem Netzwerk beitreten. Hierfür müssen sie die Software installieren. Zur Einreichung eines Artikels senden die Autor*innen ihr Manuskript über die Software an eine hierfür vorgesehene Plattform und erzeugen damit eine neue Transaktion. Die Einreichung wird mit einem Timestamp und weiteren von den Autor*innen festgelegten Metadaten, wie beispielsweise Namen (falls es kein anonymes Verfahren gibt), Speicherort des Artikeltextes und der aktuellen Version des Artikels versehen. Diese Inhalte werden dann mittels einer kollisionsresistenten Hashfunktion gehasht, was bedeutet, dass unterschiedliche Inhalte mit extrem hoher Wahrscheinlichkeit auch unterschiedliche Hashes ergeben. Empfohlen ist daher die Nutzung einer schon existierenden Hashfunktion, bei der diese Eigenschaft bewiesen ist, wie beispielsweise der schon genannte SHA-256 Algorithmus, der von der NSA entwickelt wurde.

Der Artikelinhalt selbst ist nicht Inhalt der Transaktion, aber er ist einer der Parameter, aus denen der Hash errechnet wurde. Damit kann der Inhalt durch einen Vergleich der beiden Hashes auf Authentizität geprüft werden, ohne dass man den Inhalt selbst prüfen muss. Ein Smart Contract kann dafür genutzt werden, bei jeder neuen Einreichung oder Version automatisch die Gutachter*innen zu benachrichtigen.

Die Gutachter*innen können in einem nächsten Schritt ihre Kommentare verfassen und dann eine Transaktion erzeugen. Sie können beispielsweise Kommentare in den Artikeltext schreiben, diesen dann an einer anderen Stelle abspeichern und eine neue Transaktion mit der aktualisierten Version des Artikels erzeugen oder nur die Anmerkungen in einzelnen Transaktionen übermitteln. Sinnvoll wäre es, in den Metadaten auch die vorherige Transaktion direkt zu referenzieren. Diese ist zwar ohnehin über die Chain auffindbar, eine direkte Referenz macht das Auffinden aber einfacher. Ein Smart Contract kann hierbei wieder die Autor*innen direkt über das abgegebene Feedback informieren. Dabei kann der Prozess sowohl anonym erfolgen oder unter Nennung der jeweiligen Gutachter*innen.

Weitere Feedback- und Kommentarschritte laufen analog dazu ab, so dass am Ende eine Version für Version nachvollziehbare Kette steht. Das exakte Datum sowie die Personen, die Anmerkungen oder Änderungen vorgenommen haben, sind damit stets identifizierbar, die Validität jeder einzelnen Version direkt nachvollziehbar.

Die Veröffentlichung erfolgt, wenn die Herausgeber*innen eine Transaktion erzeugen, bei der zusätzlich der Status des Artikels als »veröffentlicht« angegeben wird.

Anschließend können auch Kommentare aus der wissenschaftlichen Community nach der Veröffentlichung des Artikels in die Blockchain mit aufgenommen werden. Dies setzt voraus, dass auch die Kommentator*innen Teil des Netzwerkes werden. In einer public chain kann jedoch nicht festgelegt werden, welche Interaktionen ein Mitglied durchführen kann, weil der Grundgedanke dieser Technologie ist, dass jede*r alle Möglichkeiten der Teilnahme hat. Permissioned chains und private chains bieten hingegen die Möglichkeit, Rollen zu spezifizieren. So können etwa für Gutachter*innen und Kommentator*innen über Gruppenzuordnungen gewisse Aktionen erlaubt werden.

Auch für die Speicherung und Archivierung der Inhalte kann eine Blockchain angewendet werden, denn nach wie vor müssen die Inhalte an einer Stelle hinterlegt werden. Die Teilnehmer*innen verfügen zwar jeweils über die gleiche Chain, diese enthält aber nur die Transaktionen, nicht die Inhalte. Diese muss man separat herunterladen. Bereitgestellt werden können die Inhalte entweder über Universitätsserver oder Server der Zeitschrift, es gibt aber auch die Möglichkeit einer dezentralen Sicherung. Das bekannteste Peer-to-Peer-Dateisystem ist das InterPlanetary Filesystem (IPFS). Hierbei werden Inhalte nicht auf zentralen Servern abgelegt, sondern die Teilnehmer*innen stellen – gegen Entlohnung – Speicherplatz zur Verfügung. Das Netzwerk hält Daten mehrfach vor, damit Ausfälle einzelner Geräte kompensiert werden können. Die Inhalte liegen auch nicht in Reinform vor, sondern werden unterteilt und verschlüsselt. Eine Zuverlässigkeit, dass stets auf alle Inhalte zugegriffen werden kann, gibt es nicht, da es auch in dem Netzwerk zu Ausfällen kommen kann oder Einzelne das Netzwerk jederzeit verlassen können. Allerdings könnten sich in diesen Prozess auch Universitätsrechenzentren einbringen, und die Sicherung so auf mehrere zuverlässige Akteur*innen verteilt werden.[39] Die Frage des Hostings entfällt aber auch durch den Einsatz von Blockchain nicht.

So wie bisher geschildert, wäre der ganze Prozess von der Einreichung des Manuskriptes an öffentlich. Wenn man den Prozess bis zur Publikation aber nicht für alle – sowohl für Mitglieder des Netzwerks als auch für Außenstehende – einsehbar gestalten will, braucht man pro Artikel entweder einen Ledger oder eine private Chain, an der nur Autor*innen und die Gutachter*innen beteiligt sind.

Anstatt den ganzen Publikationsprozess mit Blockchain zu realisieren, können auch einzelne Aspekte damit implementiert werden. So könnte man beispielsweise Aspekte der Versionskontrolle und Nachverfolgung der Änderungen mit einem System wie GitHub realisieren.

[38] z.B. die C# Bitcoin Library für das .NET Framework oder das JavaScript Hyperledger Framework.
[39] Heller 2017b.

Blockchain würde man für einzelne spezifische Aufgaben nutzen. Dies betrifft vor allem die unveränderliche Dokumentation des Publikationszeitpunktes. Hierfür gibt es bereits Tools, die eingesetzt werden können. Poex ermöglicht beispielsweise die Signierung von Dateien. Es wird ein Hash der Datei erzeugt und in die Bitcoin-Blockchain geschrieben. Damit erhält die Datei einen unveränderlichen Zeitstempel. Ein weiteres Tool ist Originstamp, ein Blockchain-basierter Service, der erlaubt, einen Timestamp auf digitalen Content zu setzen, um zu sichern, seit wann ein Objekt verfügbar ist.

Es gibt mit Ledger seit 2016 eine Open Access-Zeitschrift mit Peer-Review Verfahren, die auf Blockchain fußt und die bisher drei Ausgaben veröffentlicht hat. Der thematische Fokus liegt auf Kryptowährungen und Blockchain. Autor*innen können ihre Manuskripte digital signieren, der publizierte Artikel wird dann mit Zeitstempel in der Blockchain gespeichert.

3.3 Anonymität, Identifikation, Vertrauen und Qualität – einige grundlegende Überlegungen

Noch vor technologischen Entscheidungen stellen sich drei grundlegende Fragen bei der Nutzung von Blockchain: Die nach der Anonymität und Identifizierbarkeit der Beteiligten, die nach dem Vertrauen und einer zielführenden Zusammenarbeit aller und nach der Qualitätskontrolle.

Zunächst ist zu bedenken, wie jemand in einem Blockchain-Netzwerk identifizierbar ist. Der Identifikator ist der Schlüssel, mit dem die Transaktion signiert wird. Grundsätzlich sind Personen in einem Blockchain-Netzwerk anonym. Somit kann, wenn in den Metadaten und dem Artikel kein Name genannt ist, auch das Double-Blind-Verfahren mittels Blockchain realisiert werden. Da alle Teilnehmer*innen im Netzwerk für jede einzelne Transaktion einen neuen Schlüssel nutzen können (dieser lässt sich mit der Software erzeugen), werden die Personen erst dann identifizierbar, wenn der Artikel mit Namen veröffentlicht wird. Für eine zukünftige anonyme Publikation kann dann wieder ein neuer Schlüssel genutzt werden.

Hier ist zu überlegen, ob eine vollständige Anonymität von Teilnehmer*innen in einem wissenschaftlichen Publikationsprozess gewünscht ist und auf welche Art und Weise der Nachweis erfolgt, ob es sich bei den Einreichenden auch um den genannten Autor oder die Autorin handelt.

Auch über die Frage der Identifikation hinaus stellt sich die Frage, was passiert, wenn jemand seinen privaten Schlüssel verliert. Eine andere Partei, die in den Besitz kommt, könnte mit diesem Änderungen oder Kommentare im Namen des oder der ursprünglichen Besitzer*in vollziehen, ohne dass man es unmittelbar mitbekommt oder dagegen vorgehen könnte.

Die zweite Frage ist die nach dem Vertrauen und der zielführenden Zusammenarbeit des Netzwerks bei Abwesenheit einer zentralen, ordnenden und moderierenden Instanz. Denn wenn in der Blockchain alles offen und anonym ist, ist auch nicht gewährleistet, dass alle ein für das gesamte Netzwerk positives Ziel verfolgen. Es stellt sich die ganz allgemeine Frage, ob die wissenschaftliche Community eine zentrale Mittlerrolle, die aktuell durch Universitäten, Verlage, sowie weitere Institutionen und Gruppen eingenommen wird, vollständig ersetzen will.

Auch gilt es zu klären, wie in einem dezentralen (anonymen) Netzwerk »Vertrauen« zwischen den Beteiligten entstehen kann, um gemeinschaftliche Ziele zu verfolgen.

Das Vertrauen bei Blockchain-Technologien ergibt sich aus Anreizen. Diese Anreize sollen sicherstellen, dass sich »gutes Verhalten« auszahlt, meist finanziell. Außerdem sollten negative Manipulationen aufwändig sein. So kann etwa der rechenintensive und teure Mining-Prozess bei Kryptowährungen sicherstellen, dass das System nicht missbräuchlich genutzt wird. In dem hier skizzierten Szenario fehlt solch ein direkter Anreiz in einem anonymen System.

Um missbräuchliches Verhalten, das bei gemeinschaftlicher Konsensfindung auftreten kann, anhand von Einflussmöglichkeiten einzelner Gruppen innerhalb der Blockchain zu illustrieren: Wie verhält es sich bei offenen Blockchains, wenn gewisse Gruppen, seien es einzelne Forschungsinstitute oder Vertreter*innen verschiedener »Schulen«, ein solches Netzwerk dominieren? Hier spielt auch die majority attack oder 51 % attack, [40] bei der Teilnehmer*innen, die mehr als die Hälfte des Netzwerks dominieren, dieses übernehmen können und – unter Umgehung der Konsensfindung – beliebig ändern können.

In einer nicht anonymen Community wären Manipulationen durch einzelne Akteur*innen stets sichtbar dokumentiert und blieben nachvollziehbar. Permissioned chains hingegen setzen meistens auf andere Konsensverfahren, wie Proof-of-Stake, bei denen eine solche Übernahme nicht möglich ist.

Bei permissioned blockchains stellt sich die Frage, wieso man überhaupt Blockchain einsetzt, wenn man das Netzwerk beschränken will und einer initialen Gruppe die Möglichkeit gibt zu bestimmen, wer in das Netzwerk aufgenommen wird.

Positives Verhalten im exemplarisch geschilderten Publikationsprozess könnte man etwa mittels Kryptowährung belohnen. Neben der Absicherung vor böswilliger Manipulation könnte eine solche Währung auch Anreize für Autor*innen und Gutachter*innen schaffen. Sie könnte für Autor*innen oder die Teilhabe am Begutachtungsverfahren, bei Reviews durch die

[40] Vgl. Bitcoin Wiki: Majority attack.

Community oder durch ausgesuchte Begutachter*innen, ausgezahlt werden. Die Höhe könnte beispielsweise nach einiger Zeit anhand von Häufigkeit von Downloads, Zitationen, beigefügten Forschungsdaten, Offenheit der Lizenz etc. bestimmt werden.[41]

Schließlich stellt sich noch die Frage, was der Einsatz von Blockchains im Publikationsprozess für Standards und die Sicherung von Qualität bedeutet. Zwar ändert die Art der Bereitstellung natürlich grundsätzlich nichts am Inhalt; nach wie vor gilt es, diesen durch ein wissenschaftlichen Kriterien entsprechendes Review-Verfahren sicherzustellen, dies ersetzt die Blockchain-Technologie nicht. Die Frage ist eher, ob netzwerkgetriebene Parameter, wie gemeinschaftlicher Konsens über die Qualität, zur Qualitätssicherung beitragen können. Der Einsatz von Blockchains stellt Nachvollziehbarkeit und Transparenz sicher, nicht jedoch, welcher Inhalt hinzugefügt wird.

Es ist eine daher eine Funktionalität nötig, die prüft, ob Datenänderungen sinnvoll sind und diese nur dann zulässt. Dies könnte etwa durch ein Review-Verfahren durch andere Teilnehmer*innen des Netzwerks passieren. Eine solche Funktionalität entspräche in weiten Teilen einer Neuimplementierung der Pull-Request-Funktion von GitHub.

GitHub kann als Gegenbeispiel für eine Plattform mit einem zentralen Betreiber genannt werden, der mit Hashfunktionen und Merkle tree ähnliche Technologien zugrunde liegen wie der Blockchain-Technologie. Hier wird ein Vertrauen in die Betreiber der Plattform vorausgesetzt, was insbesondere deutlich wurde, als bekannt wurde, dass Microsoft die Plattform übernimmt. Für die Akzeptanz der Plattform ist ausreichendes Vertrauen nötig, dass das Repositorium auf der Plattform bleibt und dass klar ist, wer und mit welchem Nutzerprofil die Änderungen gemacht hat. Man kann die Git-Technologie allerdings auch dezentral auf einem eigenen Server oder gehostet von einem vertrauenswürdigen Anbieter wie einem Rechenzentrum nutzen und ist damit wiederum unabhängig von einem Drittanbieter wie GitHub.

4. Fazit

Blockchain, vor zehn Jahren entwickelt, ist keine neue Technologie mehr und baut auf verschiedenen Konzepten und Technologien auf. Es gibt neben Bitcoin weitere Blockchains und Anwendungen, wobei sich viele davon im Bereich von Proof-of-Concepts bewegen.[42] Es gibt aber auch erste bereits etablierte und großteils offen verfügbare Technologien, die nachgenutzt werden können sowie verschiedene Dienste, die ihren Quellcode offen zur Verfügung stellen, wie zum Beispiel Hyperledger.[43] Diese können auch in der wissenschaftlichen Anwendung nachgenutzt werden.

Am hier dargestellten Beispiel der wissenschaftlichen Zeitschrift zeigen sich zwei wesentliche Bereiche, die es generell bei der Anwendung von Technologien in den Geisteswissenschaften zu beachten gilt: Konkrete technologische Aspekte einerseits und konzeptionelle andererseits.Hierbei stellen sich zum einen Fragen der technologischen Abwägung: Welche Schritte können sinnvollerweise mit Blockchain-Technologien umgesetzt werden? Welcher Typ von Blockchain soll eingesetzt werden, oder ist ein Ledger zielführender? Können einzelne Aspekte über andere, etablierte und niedrigschwelligere Anwendungen, wie Systeme für Versionskontrolle, realisiert werden? Gilt es beispielsweise in erster Linie Versionierbarkeit darzustellen, kann man die gewünschten Funktionalitäten auch mit Git realisieren. Bei eigenem Hosting entfällt auch hier die Abhängigkeit von einem bereitstellenden Dritten, wie der Plattform GitHub. Auch gilt es Kosten und Nutzen abzuwägen. Dies betrifft sowohl die Hürden für alle Teilnehmenden, sich die Grundlagen anzueignen, als auch die tatsächlichen Kosten, die – wenn Proof-of-Work-Verfahren eingesetzt werden – beim Mining entstehen. Außerdem muss das Netzwerk abgesichert werden und sichergestellt sein, dass böswillige Manipulationen ausgeschlossen oder zumindest minimiert werden können. Und wie bei jeder Form der Programmierung sind auch hier Fehler möglich, die zu Sicherheitslücken führen, insbesondere dann, wenn eine Blockchain nicht isoliert ist, sondern mit anderen Anwendungen interagiert. Auch die auf den Computern der Nutzer*innen gesicherten privaten Schlüssel stellen eine Angriffsfläche dar und können etwa über Trojaner abgegriffen und böswillig weiterverwendet werden.[44]

Konzeptionelle Fragen stellen sich vor allem hinsichtlich der Anonymität und Dezentralität. Der Einsatz von Blockchain fordert die Frage heraus, welche Rolle die wissenschaftliche Community, Universitäten und Verlage in diesem Netzwerk spielen können und wollen – oft sind zentrale Autoritäten auch erwünscht. Dies betrifft den Grad der Offenheit der Prozesse und der Anonymität der Beteiligten ebenso wie die Art der Konsensfindung.

Besonders wenn zentrale Instanzen fehlen, muss geklärt werden, wie Entscheidungen getroffen werden und ob dies rein konsensual geschieht oder Abstufungen vorgenommen und einzelne Entscheidungen – zum Beispiel die Entscheidung über die Qualität oder Annahme – zentralisiert werden sollen. Auch gilt es zu klären, welche Anreizsysteme geschaffen werden können, damit alle am Netzwerk Teilnehmenden diesem zuträglich verhalten. Insbesondere für diese konzeptuellen Bereiche müssen zunächst Standards etabliert werden, um Blockchain-Technologien erfolgreich einsetzen zu können. Dies kann nur durch die jeweiligen Fachcommunities erfolgen.

Insgesamt ist festzuhalten, dass der Einsatz von Blockchain kostspielig ist. Dies betrifft einerseits die Ressourcen, die es erfordert, ein solches System zu implementieren und zu betreiben, sowie andererseits den Aufwand, die Anwendung den Beteiligten in

[41] Taudes 2017.
[42] Ein Grund dafür, dass es nach wie vor wenige Anwendungen von Blockchain in der Wissenschaft gibt, ist, dass erste Implementierungen schlecht anliefen oder gescheitert sind. Vgl. dazu Heller 2017a.
[43] Hyperledger ist ein Projekt der Linux Foundation mit dem Ziel, Open Source Blockchain-Technologien bereitzustellen.
[44] vgl. Kreutzer 2018.

Theorie und Praxis verständlich zu machen. Gerade bei den beschränkteren finanziellen Mitteln in der Wissenschaft spielt das eine besondere Rolle.

Das Neue, das die Blockchain bringt, ist die Dezentralität und, in vielen ihrer Ausprägungen (s. Tabelle 1) Trustlessness, also die Unnötigkeit von Vertrauen als gemeinsamer Basis der Zusammenarbeit. Anwendungen, für die genau diese Komponenten zwingend sind, können mit Blockchain vielversprechend umgesetzt werden. In allen anderen Fällen ist die Nutzung anderer, niedrigschwelliger und etablierter Technologien und Anwendungen – wie beispielsweise Datenbanken und Git – zielführender.

Bibliographische Angaben

Sönke Bartling: Blockchain for Science and Knowledge Creation. Living Document. In: Blockchain for Science. Beitrag vom 23.02.2017. [online]

Jörn Brien: Blockchain-Technologie studieren: Diese Unis bieten das beste Angebot. In: t3n News. Karriere. Beitrag vom 12.06.2017. [online]

Anders Brownworth: Blockchain Demo. In: Anders Brownworth: Technology and Disruption. Blogbeitrag vom 30.12.2017. [online]

Guang Chen / Bing Xu / Manli Lu / Nian-Shing Chen: Exploring blockchain technology and its potential applications for education. In: Smart Learning Environments 5 (2018), H. 1. DOI: 10.1186/s40561-017-0050-x

Christoph von Eichhorn: Der Bitcoin ist angefressen. In: Technology Review Special 13 (2018), S. 71. [Nachweis im GBV]

Benedikt Fecher / Sönke Bartling: Wie Blockchain die Wissenschaft verbessern könnte. In: iRights.info. Artikel vom 06.09.2016. [online]

Sven Fund: Blockchain: Technik statt Vertrauen? In: Börsenblatt. Bookbytes. Blogbeitrag vom 11.01.2017. [online]

Alexander Grech / Anthony F. Camilleri: Blockchain in Education. Hg. von Andreia Inamorato dos Santos, Joint Research Centre (European Commission). Luxemburg 2017. (= JRC, 108255) DOI: 10.2760/60649

Mikea Hearn: Corda: A distributed ledger. Version 0.5 vom 29.11.2016. PDF. [online]

Lambert Heller (2017a): Wie P2P und Blockchain helfen, das Arbeiten mit wissenschaftlichen Objekten zu verbessern – drei Thesen. In: TIB Blog. Blogbeitrag vom 09.05.2017. [online]

Lambert Heller (2017b): Bereitstellung wissenschaftlicher Objekte mittels Smart Contracts auf einer Blockchain – wie und warum? In: TIB Blog. Blogbeitrag vom 03.06.2017. [online]

Ekki Kern: Blockchain soll 2018 das Internet der Dinge revolutionieren. In: t3n News. Software & Infrastruktur. Beitrag vom 15.12.2017. [online]

Sunny King / Scot Nadal: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 19.08.2012. PDF. [online]

Michael Kreutzer: Darum könnte die Bitcoin-Technologie ein gefährliches Sicherheitsrisiko für die ganze Wirtschaft sein. In: Businessinsider. Beitrag vom 26.02.2018. [online]

Andreas Lenz: Blase? Nein! Warum Bitcoin und Blockchain die nächste Evolutionsstufe des Internets sind. In: t3n News. Digitale Wirtschaft. Beitrag vom 14.12.2017. [online]

Christoph Meinel / Tatiana Gayvoronskaya / Maxim Schnjakin: Blockchain: Hype oder Innovation. Potsdam 2018. URN: urn:nbn:de:kobv:517-opus4-103141 [Nachweis im GBV]

Ralph Charles Merkle: A digital signature based on a conventional encryption function. In: Advances in Cryptology — CRYPTO '87. Proceeding. Hrsg. von Carl Pomerance. (Crypto: 7, Santa Barbara, CA, 16.-20.08.1987) Berlin u.a. 1988, S. 369-378. [Nachweis im GBV]

Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. PDF. [online]

Yuji Nakamura / Lulu Yilun Chen: Bitcoin Miners Signal Revolt Amid Sluggish Blockchain, In: Bloomberg. Artikel vom 13.03.2017. [online]

Arvid Narayanan / Joseph Bonneau / Edward Felten / Andrew Miller / Steven Goldfeder: Bitcoin and Cryptocurrency Technologies. A comprehensive Introduction. Princeton 2016. [Nachweis im GBV]

Joris van Rossum: Blockchain for Research. Perspectives on a New Paradigm for Scholarly Communication. London 2017. DOI: 10.6084/m9.figshare.5607778

Vincent Schlatt / André Schweizer / Nils Urbach / Gilbert Fridgen: Blockchain: Grundlagen, Anwendungen und Potenziale. Discussion Paper. Hg. vom Fraunhofer FIT. Augsburg 2016. PDF. [online]

Sven Slootweg: Is my blockchain a blockchain? In: GitHub.com. Beitrag (joepie91) vom 25.11.2016. [online]

Florian Süssenguth / Anna-Laura Liebenstund: Blockchain. Hrsg. von Acatech - Deutsche Akademie der Technikwissenschaften. München u.a. 2018. (= Acatech Horizonte, 1) [online]

Alfred Taudes: Peer-to-Peer-Wissenschaftsverlage funktionieren nicht - oder doch? In: Der Standard. Blog: Kryptoökonomie. Blogbeitrag vom 14.12.2017. [online]

Janna Tillmann: Naivechain: Blockchain in nur 200 Zeilen Javscript-Code. In: t3n News. Entwicklung & Design. Beitrag vom 22.04.2018. [online]

John Wiegley: Ledger. In: GitHub.com. Erste veröffentlichte stabile Version 1.1 vom 13.02.2004. [online]

Webseiten

About pull requests. In: GitHub Help. [online]

Bitcoin Energy Consumption Index. [online]

Bitcoin Mining in China. [online]

Bitcoin Mining Pools. [online]

Blockchain-Labor des Fraunhofer-Instituts für Angewandte Informationstechnik. [online]

Blockchain Competence Center der HS Mittweida. [online]

Blockchain Research Cluster der TU München. [online]

Center for Distributed Ledgers and Contracts der TU Darmstadt. [online]

Consensus - R3 Corda V3.0 documentation. [online]

Composer. In: GitHub. [online]

Corda. [online]

Cypherpunk. In: Wikipedia. [online]

The DAO (Organization). In: Wikipedia. [online]

Ethereum. [online]

Flyer zum Studiengang "Blockchain & Distributed Ledger Technologies (DLT)" der HS Mittweida. PDF. [online]

Futurice Spice Program. [online]

Hyperledger. [online]

Hyperledger Framework. In: GitHub. [online]

InterPlanetary File System. [online]

Ledger. [online]

Ledgerjournal. [online]

Majority Attack. In: Bitcoin Wiki. [online]

Nbitcoin. In: GitHub. [online]

Originstamp. [online]

Poex.io. [online]

P wie Publizieren. In: Zeitschrift für digitale Geisteswissenschaften – ZfdG. [online]

SHA-2. In: Wikipedia. Letzte Änderung: 26.7.2018. [online]

Steemit. [online]

Abbildungslegenden und -nachweise

Abb. 1: Block bestehend aus Header und Transaktionsdaten. [Anna Neovesky / Julius Peinelt 2018. CC BY 4.0.]

Abb. 2: Blöcke in der Blockchain mit dem aktuellen Branch, dem Main Branch und nicht mehr weiterverfolgten Branches. [Anna Neovesky / Julius Peinelt 2018. CC BY 4.0.]

Abb. 3: Schema eines Merkle tree. [Anna Neovesky / Julius Peinelt 2018, aufbauend auf Hash Tree von Becky In: bitcoinwiki 2018. CC BY 4.0.]

Abb. 4: Vereinfachte Darstellung des Ablaufs einer Transaktion. [Anna Neovesky / Julius Peinelt 2018. CC BY 4.0.]