STIFTERVERBAND
Bildung. Wissenschaft. Innovation.

VDI Technologiezentrum

Grundlagen – Potenziale – Grenzen

BLOCKCHAIN IN DER HOCHSCHULBILDUNG

Anthony F. Camilleri | Thomas Werner | Andreas Hoffknecht | Andreas Sorge

BEAUFTRAGT VOM

Bundesministerium
für Bildung
und Forschung

INHALT

VORBEMERKUNG 04

01 EINLEITUNG 06

02 TECHNISCHE UND KONZEPTIONELLE GRUNDLAGEN DER BLOCKCHAIN 09

2.1 Verteilte Systeme 09
2.2 Vertrauen und Integrität in verteilten Systemen 12
2.3 Identität, Eigentum und Eigentumsverwaltung 13
2.4 Hash-Funktionen 15
2.5 Asymmetrische Kryptografie als Grundlage der Blockchain 21
2.6 Blockchain als Datenspeicher 25
2.7 Einfügen und Überprüfen von Transaktionen 28
2.8 Kosten zur Aufrechterhaltung der Integrität 31
2.9 Spieltheorie und Incentivierung 36

03 DER SOZIOTECHNISCHE CHARAKTER DER BLOCKCHAIN 39

3.1 Technische Eigenschaften von Blockchain-Anwendungen 40
3.2 Soziotechnische Beschränkungen der Blockchain 41
3.2.1 Technische Beschränkungen 41
3.2.2 Beschränkungen der Blockchain im Kontext der DSGVO 42
3.2.3 Sozioökonomische Beschränkungen der Blockchain 44
3.3 Soziotechnische Mehrwerte der Blockchain 46
3.3.1 Gesellschaftliche Werte und Allgemeinnutzen 46
3.3.2 Technische Errungenschaften 46
3.4 Nachteile der Blockchain 47
3.5 Elementare Anwendungen 49
3.6 Prominente Blockchain-Projekte und Architekturen 50
3.6.1 Marktüberblick 50
3.6.2 Bitcoin (BTC) als archetypische Blockchain-Anwendung 54
3.6.3 Ethereum (ETH) und Smart Contracts 55
3.6.4 Dezentralisierte Anwendungen (dApps) und Dezentralisierte Autonome Organisationen (DAOs) 56
3.6.5 Hyperledger 56
3.6.6 Weitere branchenspezifische Blockchain-Projekte 57

3.7 Soziotechnische Typen von Blockchains 62
3.7.1 Offene, geschlossene und hybride Blockchain-Architekturen 62
3.7.2 Öffentliche und private Blockchains 63
3.7.3 Genehmigungsfreie und genehmigungspflichtige Blockchains (permissionless blockchains vs. permissioned blockchains) 64
3.8 Abwandlungen, Weiterentwicklungen, Alternativen 65
3.8.1 Forks von Blockchains 65
3.8.2 Konsensverfahren 67
3.8.3 Weitere Entwicklungspfade der Blockchain-Technologie 68
3.8.4 Ausgestaltung der Blockchain-Technologie für Anwendungen 70
3.9 Forschungsfragen 70

04 EINSATZ DER BLOCKCHAIN-TECHNOLOGIE IM HOCHSCHULBILDUNGSSYSTEM 75

4.1 Spezifische Rahmenbedingungen für den Einsatz der Blockchain-Technologie im deutschen Hochschulbildungssystem 75
4.2 Szenarien des Einsatzes und Anwendungsfälle von Blockchain im Hochschulbildungsbereich 76
4.3 Bildungsnachweise beglaubigen, ausstellen und anerkennen 78
4.3.1 Hintergrund 78
4.3.2 Ausgangslage 80
4.3.3 Beschreibung von Methoden zur Anwendung von Blockchain-Technologie 82
4.3.4 Potenziale des Einsatzes von Blockchain 82
4.3.5 Ausstellung beglaubigter Bildungsnachweise 84
4.3.6 Verifizierung von Zertifikaten 84
4.3.7 Verifizierte digitale Identitäten für Hochschulen 84
4.3.8 Automatische Übertragung und Akkumulierung von Studienleistungen (Credits) 85
4.3.9 Teilen und Verifizieren von Nachweisen erfahrungsbasierter Kompetenzen 86
4.3.10 Analyse 87
4.4 Software und Daten in Lehre und Studium dezentralisieren 88
4.4.1 Hintergrund und Ausgangslage 88
4.4.2 Dezentralisierte Anwendungen und ihre Potenziale 90
4.4.3 Dezentralisierte Social Apps für den Bildungsbereich 90
4.4.4 Analyse 90
4.5 Studierendendaten in der Verwaltung minimieren 91
4.5.1 Hintergrund 91

4.5.2 Ausgangslage 91
4.5.3 Einsatz und Potenzial der Blockchain 92
4.5.4 Management der Studierendenidentität im Hochschulbildungssystem 93
4.5.5 Analyse 93
4.6 Akademische Inhalte und Werke nachverfolgen 94
4.6.1 Hintergrund 94
4.6.2 Ausgangslage 95
4.6.3 Einsatz und Potenzial der Blockchain 95
4.6.4 Beglaubigung von Autorenschaften und IP-Rechten 96
4.6.5 Nachverfolgung der Nutzung von akademischen Inhalten und Werken 96
4.6.6 Analyse 96
4.7 Zahlungen und Mittelflüsse managen 97
4.7.1 Hintergrund und Ausgangslage 97
4.7.2 Einsatz und Potenzial der Blockchain 99
4.7.3 Zahlung von Studiengebühren 99
4.7.4 Studienförderung 99
4.7.5 Leistungsbezogene Mittelzuweisung 99
4.7.6 Analyse 100
4.8 Weitere Szenarien 101
4.8.1 Wahlen 101
4.8.2 Dezentralisierte Autonome Organisationen 101
4.8.3 Integration in den gesamten Forschungsprozess 101
4.8.4 Prüfungen 102
4.9 Einschätzungen von Stakeholdern und Experten 102
4.9.1 Diskussionen mit Stakeholdern in Deutschland 102
4.9.2 Interviews mit internationalen Experten 105

ANHANG 109

Literaturverzeichnis 109
Abbildungsverzeichnis 117
Tabellenverzeichnis 118
Verzeichnis der Einsatzszenarien von Blockchain im Hochschulbildungsbereich 119
Verschlagwortete Literatur 120
Initiativen im Bereich Blockchain in der Hochschulbildung 120
Checkliste für Anforderungen an den Einsatz von Blockchain 123

VORBEMERKUNG

Blockchain gilt als Zukunftstechnologie mit hohem disruptivem Potenzial, um über das Internet Werte, Vereinbarungen oder Transaktionen ohne zentrale Instanz vertrauenswürdig austauschen zu können. Der Diskurs zu ihrem Einsatz im deutschen Hochschulsystem im digitalen Zeitalter ist vielversprechend, facettenreich und entwickelt sich – auch und gerade im europäischen Kontext – rasant. Dieser Bericht ist eine Bestandsaufnahme zu einer Zeit, da sich auch in Deutschland Anbieter, Netzwerke und Kooperationen formieren, die Lösungsansätze für den Blockchain-Einsatz vorbereiten und entwickeln. Nicht zuletzt gilt es, vor dem Hintergrund standortbezogener Wettbewerbsszenarien auch die internationale Strahlkraft und den Startvorteil Deutschlands mit Berlin als europäischen und international Talente attrahierenden Hub der internationalen Blockchain-Entwickler- und Start-up-Community zu stärken. Ihre Entwicklungen sind nicht nur wirtschaftlich verwertbare Innovationen, sondern auch für soziale, gemeinwohlorientierte Innovationen nutzbar. Dieser Bericht knüpft an die Ende 2017 veröffentlichte EU-Studie „Blockchain in Education“ unmittelbar an, führt die dort enthaltenen Ansätze fort und diskutiert sie im Kontext des deutschen Hochschulbildungssystems.

Der vorliegende Bericht versucht, das Spannungsfeld zwischen tagesaktueller Politikberatung und langfristigen sozioökonomischen Implikationen der Blockchain-Technologie für das Hochschulbildungssystem zu diesem günstigen Zeitpunkt produktiv aufzulösen. Hierzu beschreiben die einzelnen Kapitel die vergleichsweise allgemeinen technologischen Grundlagen der Blockchain-Technologie und die technischen, ökonomischen und gesellschaftlichen Mehrwerte und Risiken ihres Einsatzes. Diese werden sodann verdeutlicht und geschärft anhand der Darstellung, Bewertung und Diskussion von Anwendungsszenarien mit konkreten Anwendungsfällen im Hochschulbildungsbereich. Es wird immer wieder deutlich werden, dass der Einsatz von Blockchain vielen Unwägbarkeiten unterliegt und sowohl technisch als auch aus Governance-Perspektive wohlinformiert gestaltet werden muss, um den gewünschten gesellschaftlichen Nutzen zu erzielen.

Die Autoren möchten mit diesem Bericht einen Beitrag dazu leisten, Blockchain kritisch abgewogen und zugleich agil zum allgemeinen Nutzen im Hochschulbildungssystem kurz- und mittelfristig einzusetzen. Die Autoren erwarten von diesem Bericht, dass er Entscheidungsträgern, Innovatoren und Experten im Hochschulbildungssystem eine gemeinsame Diskursgrundlage, Aha-Momente, Einsichten, Leitlinien wie Inspiration für die weitere kritische Auseinandersetzung mit Blockchain und ihrem Einsatz bietet. Zugleich zeigt der Bericht Ansätze auf, wie im Sinne von Offener Wissenschaft und Innovation und einer Kultur der Offenheit für Experimente Blockchain im deutschen Hochschulbildungssystem entwickelt, getestet und zielorientiert zum Einsatz gebracht werden kann.

01

EINLEITUNG

Blockchain in der Hochschulbildung einzusetzen, ist ein so komplexes wie vielversprechend erscheinendes Unterfangen. Die von der EU beauftragte Studie Blockchain in Education (vgl. Grech/Camilleri, 2017) entwickelt Prinzipien, die dem gesellschaftlichen Nutzenversprechen (social value proposition) der Blockchain-Technologie für das Hochschulbildungssystem zugrunde liegen. In der EU-Studie wird dargelegt, welche Chancen durch die Blockchain für die Weiterentwicklung des deutschen sowie des gesamten europäischen Hochschulraums bestehen. Dieser Bericht knüpft daran an und bespricht auf Grundlage einer umfangreichen Literaturanalyse (siehe Anhang) zunächst die technischen und ökonomischen Grundlagen der Blockchain, um derart informiert die Blockchain-Technologie und ihre verschiedenen Ausprägungen in den gesellschaftlichen Kontext zu stellen und in verschiedenen Anwendungsgebieten kritisch zu diskutieren. Auf Basis der aufgearbeiteten Anwendungsbeispiele wird beschrieben, wie die Blockchain bestehende Arbeits-, Geschäfts- oder Verwaltungsprozesse verändern kann. Anhand dieser Einsatzmöglichkeiten und aufbauend auf der EU-Studie werden Einsatzszenarien von Blockchain im Hochschulbildungsbereich entwickelt. Im Mittelpunkt stehen insbesondere solche Szenarien, die kurz- bis mittelfristig einen hohen Impact für die Weiterentwicklung von hochschulübergreifenden Strukturen erwarten lassen. Alle aufgeführten Szenarien sind dabei prinzipiell sowohl auf das grundständige Studium wie auf die wissenschaftliche Weiterbildung anwendbar. Aus den Szenarien und den soziotechnischen Merkmalen der Blockchain lassen sich schließlich Richtlinien und Empfehlungen für Hochschulen und Politik ableiten. Bevor im Folgenden der Aufbau und die einzelnen Kapitel dieses Berichts näher dargestellt werden, wenden wir uns zunächst einer gängigen technischen Definition einer Blockchain zu:

> „Technisch gesehen ist eine Blockchain eine dezentrale, auf vielen Computern verteilte Datenbank, mit der Aufzeichnungen von Transaktionen hinterlegt werden, die für jeden Teilnehmer dieser Blockchain einsehbar sind. Die Computer, die an einer Blockchain teilnehmen, sind über das Internet vernetzt und bilden damit ein Blockchain-Netzwerk. In jeden neuen Datensatz (‚block') wird eine kryptografische

> Prüfsumme (Hashwert) der bisherigen Kette (‚chain') von Datensätzen geschrieben, sodass eine Manipulation der Daten durch einzelne Teilnehmer im Prinzip unmöglich ist. Jeder neue Block wird durch ein dezentrales Konsensverfahren geschaffen und an die Blockchain angehängt, durch das die Reihenfolge der Datensätze in der Blockchain festgelegt wird." (VDI Technologiezentrum, 2018)

Die in der Definition verwendeten Begriffe werden im Folgenden aufgegriffen, die hinter der Blockchain stehenden Technologien und Konzepte erklärt und sukzessive ein Gesamtbild erzeugt, mit dem deutlich wird, wie präzise die einzelnen Komponenten einer Blockchain aufeinander abgestimmt sind. Da fälschlicherweise oft von *der* Blockchain gesprochen wird, ist es zielführend, die ursprüngliche, erste und heute noch größte Blockchain (Bitcoin) als Verständnisgrundlage zu erörtern. Parallel wird auf notwendige Varianten, Erweiterungen und Derivate eingegangen. Im Anschluss sollen ein Ausblick gegeben und über Anwendungsbeispiele aus den verschiedensten Bereichen dieser Varianten inklusive Chancen und Risiken reflektiert werden.

Das Kapitel 2 *Technische und konzeptionelle Grundlagen der Blockchain* erläutert zunächst diese technischen und konzeptionellen Grundlagen der Blockchain. Zu diesen zählen neben verteilten Systemen und den Prinzipien von Vertrauen und Integrität in verteilten Systemen auch das Verständnis und der Datenspeicher, daher sollen das Einfügen und Überprüfen von Operationen auf der Blockchain (also zum Beispiel das Verschieben von Eigentum und anderen Transaktionen) im Detail betrachtet werden. Insbesondere wird auf die Konsensbildung in verteilten Systemen beziehungsweise bei Transaktionen auf der Blockchain Wert gelegt. Das Kapitel *Technische und konzeptionelle Grundlagen der Blockchain* stellt zudem die Aufrechterhaltung der Integrität und die Incentivierung der Teilnehmer dar. Es wird sich zeigen, dass je nach Anwendung antagonistische Ziele bei Betreibern, aber auch Teilnehmern vorherrschen und wie die Blockchain-Infrastruktur ohne administrativen Einfluss selbstregulierend diese antagonistischen Ziele austariert und das System permanent zur Sicherstellung der Integrität nachjustiert.

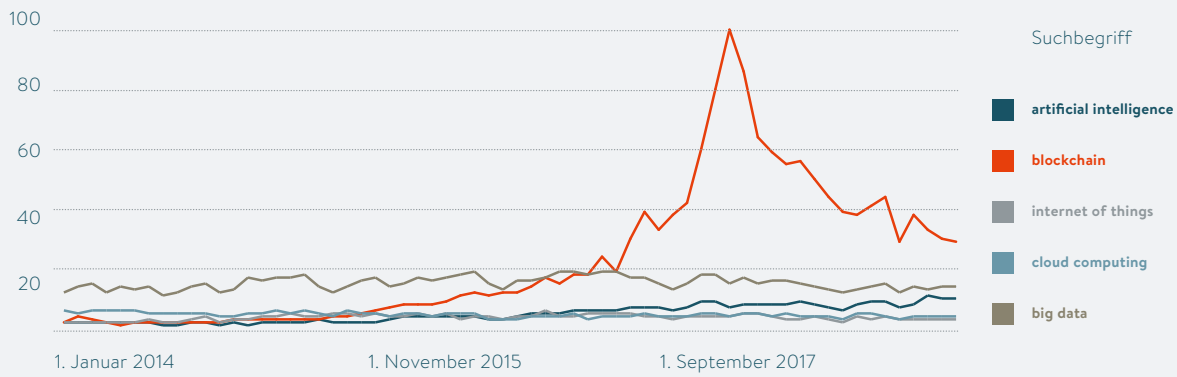
Das Kapitel 3 *Der soziotechnische Charakter der Blockchain* erörtert Merkmale, Eigenschaften, Errungenschaften, aber auch Nachteile der Blockchain. So führen Unveränderlichkeit, Robustheit und Autonomie dazu, dass ein solches System technisch und konzeptionell gegebenenfalls auf eine Betriebszeit von vielen Jahrzehnten ausgelegt sein muss. Aus diesen Überlegungen ergeben sich schnell den Einsatz einer Blockchain beschränkende Faktoren wie begrenzte Skalierbarkeit, hohe Kosten und, bei Verzicht von Intermediären, das Entstehen einer für den Benutzer ungewohnten Selbstverantwortung. Ebenfalls werden typische Blockchain-Anwendungen (zum Beispiel der Nachweis der Identität, des Eigentums oder der Nachweis einer Urheberschaft), Anwendungsfelder und beispielhaft konkrete kommerzielle Beispiele erläutert. Das Kapitel *Der soziotechnische Charakter der Blockchain* schließt mit aktuellen Weiterentwicklungen, Modifikationen und Alternativen zur Blockchain und greift Fragen zur Anforderungsgestaltung auf.

Das Kapitel 4 *Einsatz der Blockchain-Technologie im Hochschulbildungssystem* beleuchtet das Potenzial der Anwendung von Blockchain-Technologie auf dem Feld der Hochschulbildung. In diesem Kontext werden bei der Analyse der Gegebenheiten in Deutschland im Hinblick auf geeignete Anwendungsmöglichkeiten die besonderen Merkmale berücksichtigt und Szenarien für den Einsatz von Blockchain-Technologie im Hochschulbildungssystem beschrieben und analysiert. Zugleich werden die Erkenntnisse und Bewertungen von Stakeholdern im deutschen Hochschulbildungssystem zu den Szenarien und von ausgewählten internationalen Experten für den Einsatz von Blockchain-Technologie in der Hochschulbildung dargestellt.

EXKURS: ZUM ÖFFENTLICHEN DISKURS ZUR BLOCKCHAIN

ABBILDUNG 1: GOOGLE-SUCHANFRAGENVERLAUF ZU POPULÄREN IT-THEMEN

Januar 2014 bis April 2019



Quelle: Google 2019. Abgerufen am 29.05.2019 von https://trends.google.de/trends/explore?date=2014-01-01%20 2019-04-30&geo=DE&q=artificial%20intelligence,blockchain,internet%20of%20things,cloud%20computing,big%20data

Kaum ein Technologie-Thema hat in den vergangenen Jahren die Medien und das Interesse so sehr bestimmt wie das Thema Blockchain. Nach einer weltweiten Umfrage der englischen Großbank Hongkong & Shanghai Banking Corporation Holdings aus dem Jahr 2017 haben rund 40 Prozent aller Befragten schon einmal von Blockchain gehört, gleichzeitig gaben 80 Prozent, die davon gehört haben, an, nicht zu verstehen, was Blockchain ist und wie sie funktioniert (vgl. Hongkong & Shanghai Banking Corporation Holdings PLC/HSBC, 2017).

Blockchain wird mit Bitcoin und anderen „dubiosen digitalen Währungen", den sogenannten Kryptowährungen, gleichgesetzt. Diese sind oft negativ konnotiert, da sie vermeintlich zur Bezahlung illegaler Aktivitäten im Dark Web (vgl. Ryte Wiki, 2019) eingesetzt werden. So gaben bei einer 2017 durch das britische Meinungsforschungsinstitut YouGov (vgl. YouGov, 2017) durchgeführten Meinungsumfrage über 60 Prozent der befragten Amerikaner an, dass Kryptowährungen primär für illegale Geschäfte eingesetzt werden (vgl. Fanusie/Robinson, 2018). Wenn man den verschiedenen kursierenden Definitionen von Blockchain Glauben schenkt, ist die Blockchain, je nach Quelle, anonym, aber gleichzeitig offen und transparent, sie ist sicher, aber auch ständigen Angriffen ausgesetzt. Die Blockchain unterliegt permanenten Anpassungen und Justierungen, obwohl sie doch eigentlich unveränderlich ist. Sie soll effizient und kosteneinsparend sein und gleichzeitig soll die bekannteste Blockchain der Kryptowährung Bitcoin so viel Strom wie ganze Staaten – wie Österreich, Belgien und die Schweiz zusammengenommen – benötigen (vgl. Digiconomist, 2019; Lexas Länderdaten, 2019). Die Blockchain soll dezentral sein und gleichzeitig beherrscht zum Beispiel China zu mehr als 70 Prozent den Markt der Bitcoin-Blockchain (vgl. Buy Bitcoin Worldwide, 2019). Blockchain wird als „disruptive Technologie" bezeichnet und doch sind die in der Blockchain verwendeten und miteinander verbundenen Technologien schon seit Jahrzehnten in der Informatik bekannt und im Einsatz.

Die Darstellung von aktuellen Anwendungen und zukünftigen Einsatzmöglichkeiten der Blockchain-Technologie erscheint sehr unübersichtlich und häufig widersprüchlich. Eine Klärung wird insbesondere dadurch erschwert, dass die augenscheinlich ambivalenten Teilaspekte in zahlreichen Medien immer wieder isoliert wiederholt werden. Dieser Umstand überrascht nicht, gibt es doch bis heute keine eindeutige, allgemein anerkannte Definition des Begriffs Blockchain und jene Definitionen, die sich durchgesetzt haben, scheinen eher eine Aneinanderreihung von zwar korrekten, aber schwer greifbaren Umschreibungen zu sein. Dieser Bericht soll einen Beitrag dazu leisten, die verschiedenen Begriffe zu ordnen und Widersprüche zu adressieren, und so den weiteren Diskurs zu informieren.

02

TECHNISCHE UND KONZEPTIONELLE GRUNDLAGEN DER BLOCKCHAIN

2.1 Verteilte Systeme

ZUSAMMENFASSUNG

» **Verteilte Systeme stellen einen gegensätzlichen Ansatz gegenüber der klassischen Client-Server-Architektur dar. Technisch gesehen bieten sie eine höhere Ausfallsicherheit und skalieren besser, aber die Kosten für Entwurf und Kommunikation sind aufgrund der verteilten Natur und Komplexität höher.**

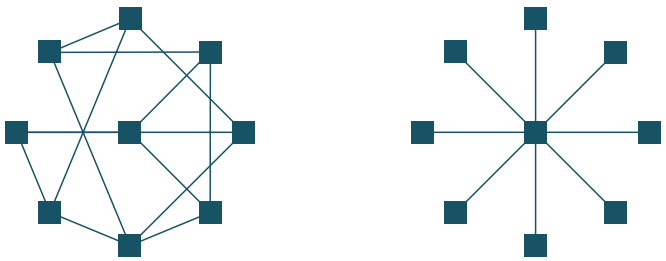
> „Technisch gesehen ist eine Blockchain eine dezentrale, auf vielen Computern verteilte Datenbank, mit [sic!] der Aufzeichnungen von Transaktionen hinterlegt werden […].“ (VDI Technologiezentrum, 2018, S. 2)

VERTEILTE SYSTEME VS. ZENTRALISIERTE ARCHITEKTUREN

Gemäß Tanenbaum und van Steen gibt es zwei fundamentale Ansätze, Software-Architekturen zu entwerfen und damit festzulegen, wie die einzelnen Komponenten eines Systems zueinander organisiert sind (vgl. Tanenbaum/van Steen, 2007). Abbildung 2 zeigt diese beiden gegensätzlichen Architekturen. Rechts ist eine zentralisierte Architektur zu sehen, in der jede Komponente des Systems (zum Beispiel ein Computer oder auch die Komponenten eines Computers) mit einer zentralen Komponente verbunden ist, es gibt keine direkten Verbindungen der Komponenten außer über das Zentrum. Links ist eine dezentrale oder verteilte Architektur dargestellt, bei der alle Komponenten untereinander ohne zentrales Element verbunden sind.

ABBILDUNG 2: VERTEILTE ARCHITEKTUR (LINKS), ZENTRALISIERTE ARCHITEKTUR (RECHTS)

Während bei der zentralisierten Architektur jede Komponente mit einer zentralen Komponente verbunden ist, sind in einer dezentralen Architektur alle Komponenten miteinander verbunden – ganz ohne zentrales Element.



Quelle: Eigene Darstellung

Gegenüber Einzelcomputern bietet ein verteiltes System verschiedene Vorteile. Die Rechenleistung im Verbund, also in einem verteilten System, ist üblicherweise höher (auch wenn die Leistung nicht linear mit der Anzahl der Komponenten skaliert) als bei Einzelcomputern. Temporär ungenutzte Ressourcen wie beispielsweise Speicherplatz können im Verbund besser ausgelastet werden. Wie in Abbildung 2 zu erkennen ist, können einzelne Komponenten (oder Pfade/Verbindungen) des Systems entfernt werden und trotzdem sind die restlichen Komponenten des Verbundes über Alternativpfade zu erreichen. Das heißt, in einem verteilten System gibt es keine Komponente, deren Ausfall zum Versagen des Gesamtsystems führt, wodurch die Zuverlässigkeit des Systems höher ist als bei isolierten oder bei zentralisierten Systemen (bei zentralisierten Systemen ist vor allem die zentrale Komponente ein kritisches Element).

VERTEILUNG VON RESSOURCEN

Verteilte Systeme skalieren besser als zentralisierte Architekturen, das heißt, dass die Systemleistung hier sukzessive durch Hinzufügen neuer Komponenten gesteigert werden kann. Dem gegenüber stehen aber auch Nachteile. So ist der Aufwand der Koordinierung deutlich größer. Durch das Fehlen einer zentralen Instanz muss ein verteiltes System inhärent administriert werden, das heißt, für die Koordinierung ist nicht nur ein austariertes Konzept, sondern sind auch die Teilnehmer des Systems verantwortlich. Damit einher geht ein deutlich höherer Aufwand für die Kommunikation. Während in einem zentralen System die zentrale Komponente die Koordinierung übernimmt, muss in verteilten Systemen die Koordinierung vor allem über die Kommunikation der Teilnehmer/Komponenten untereinander stattfinden. Dies verursacht Kosten und zudem eine Abhängigkeit vom zugrundeliegenden Kommunikationsnetzwerk. Ohne Netzwerk kann keine Kommunikation stattfinden und dadurch ein verteiltes System nicht mehr funktionieren. Verteilte Systeme sind zudem aufgrund ihrer Komplexität in der Entwicklung teurer (sowohl in der Programmierung, beim Test und der Qualitätssicherung als auch im Betrieb).

SKALIERUNG VERTEILTER SYSTEME

HOHER KOMMUNIKATIONS-AUFWAND

Eine besondere Form von verteilten Systemen stellen Peer-to-Peer-Netze dar. In einem (rein verteilten) Peer-to-Peer-Netz sind alle beteiligten Computer (Knoten) gleichberechtigt und können sowohl Ressourcen (zum Beispiel Rechenleistung, Speicherplatz oder Netzbandbreite) in Anspruch nehmen als auch zur Verfügung

PEER-TO-PEER-NETZE

stellen. Peer-to-Peer-Netze werden daher häufig als „Netzwerk von Gleichberechtigten“ bezeichnet. Die Knoten sind bezüglich ihrer Rollen und Rechte im System identisch, es gibt keine zentrale Koordinierungsstelle oder exponierte Knoten. Zusammen mit der Skalierungsfähigkeit verteilter Systeme wächst damit auch die Leistungsfähigkeit eines solchen Systems, denn durch das Hinzufügen neuer Knoten stehen weitere Systemressourcen bereit, wohingegen beim Client-Server-Modell in erster Linie der Server zentral aufgerüstet werden muss.

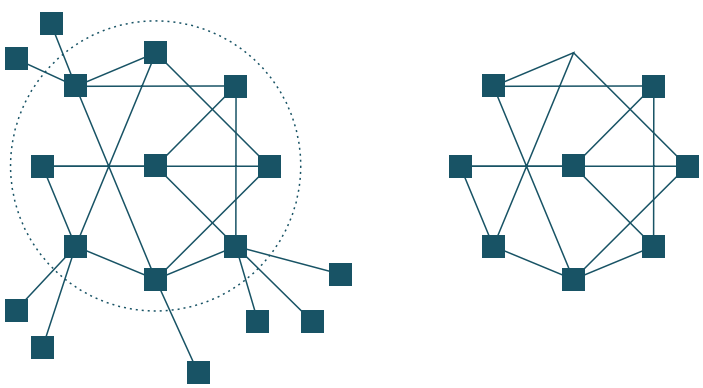
↖ CLIENT-SERVER-ARCHITEKTUR

Verteilte und zentralisierte Systeme sind von ihrer Architektur her gegensätzlich, doch wie in anderen Bereichen auch neigen in der Software-Technik die Entwickler dazu, die Vorteile verschiedener Systeme zu einem neuen System zu vereinen. So werden verteilte Systeme mit zentralen Komponenten entworfen, aber auch zentralisierte Systeme mit verteilten Komponenten. Abbildung 3 zeigt solche Architekturen. Bei diesen Mischformen oder auch Hybridarchitekturen ist es häufig schwierig festzustellen, um welche Art von System es sich handelt. Zur Vereinfachung kann Folgendes festgelegt werden: Wenn eine beliebige Komponente aus dem Netzwerk entfernt wird und das Gesamtsystem so nicht funktioniert, handelt es sich nicht mehr um ein verteiltes System. Dennoch sind zentralisierte Peer-to-Peer-Systeme häufig dort anzutreffen, wo ein administrierender Einfluss notwendig oder erwünscht ist. Beispielsweise verwaltete die Musiktauschbörse Napster (vgl. Wikipedia, 2019) über eine zentrale Datenbank alle mit dem Peer-to-Peer-System verbundenen Knoten sowie die auf den Knoten gespeicherten Inhalte. Der eben gezeigten Definition nach entspricht diese Anordnung also einer Hybridarchitektur.

↖ HYBRID-ARCHITEKTUREN

ABBILDUNG 3: HYBRIDARCHITEKTUR

Links die Zentralisierung um einen Kern, der verteilt aufgebaut ist; rechts eine Architektur, die nicht mehr ausfallsicher ist, sobald der Zentralknoten entfernt wird



Quelle: Eigene Darstellung

Rein verteilte Peer-to-Peer-Systeme führen zur Disintermediation,[1] da mit der Gleichstellung der Teilnehmer in einem Peer-to-Peer-Netz die Interaktion naturgemäß direkt zwischen den Teilnehmern ohne vermittelnde Instanz stattfindet. Der Einsatz von rein verteilten Peer-to-Peer-Netzen stellt daher für viele Unternehmen, deren Geschäftsmodell hauptsächlich die Vermittlung unter Teilnehmern ist, eine Bedrohung ihres Geschäftsmodells dar. Beispielsweise können Autoren ihre Bücher heute direkt

↖ REIN VERTEILTE PEER-TO-PEER-SYSTEME

↖ DISINTERMEDIATION

als E-Book vertreiben, ohne auf einen Verlag angewiesen zu sein, und Hersteller haben die Möglichkeit zum Direktvertrieb über den eigenen Onlineshop, was zu einer Disintermediation der klassischen Handelsstrukturen führt. Die in den folgenden Kapiteln dargestellten technischen Grundlagen der Blockchain orientieren sich an der ältesten heute noch im Einsatz befindlichen Blockchain, die tatsächlich als rein verteiltes Peer-to-Peer-System entworfen wurde.

2.2 Vertrauen und Integrität in verteilten Systemen

ZUSAMMENFASSUNG

» **2008 erschien unter dem Pseudonym Satoshi Nakamoto ein Dokument, in dem konzeptionell und technisch ein öffentliches verteiltes Hauptbuch für Transaktionen beschrieben wurde, bei denen trotz unbekannter Teilnehmer Vertrauen und Integrität in einem verteilten System gewährleistet werden können.**

Um zu verstehen, wie eine Blockchain Integrität und Vertrauen in einem Netzwerk unbekannter Zuverlässigkeit, mit unbekannten Teilnehmern und unbekannter Vertrauenswürdigkeit schafft, lohnt ein detaillierter Blick auf die Bitcoin-Blockchain, die bis heute die älteste und bekannteste Blockchain darstellt.

> „Technisch gesehen ist eine Blockchain eine dezentrale, auf vielen Computern verteilte Datenbank, mit der Aufzeichnungen von Transaktionen hinterlegt werden, die für jeden Teilnehmer dieser Blockchain einsehbar sind. Die Computer, die an einer Blockchain teilnehmen, sind über das Internet vernetzt und bilden damit ein Blockchain-Netzwerk." (VDI Technologiezentrum, 2018, S. 2)

INTEGRITÄT, VERFÜGBARKEIT UND VERTRAULICHKEIT

Die Aufrechterhaltung der Integrität ist neben Verfügbarkeit und Vertraulichkeit eines der drei klassischen Ziele der Informationssicherheit und damit eine der Kernaufgaben eines jeden Softwaresystems. Das Bundesamt für Sicherheit in der Informationstechnik schreibt hierzu:

> „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf ‚Daten' angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf ‚Informationen' angewendet. Der Begriff ‚Information' wird dabei für ‚Daten' verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden." (Bundesamt für Sicherheit in der Informationstechnik, 2019)

VERTRAUEN IN DIE WAHRHEIT EINES SYSTEMS

Das System und damit die dort verarbeiteten Daten sollen korrekt, sicher, einheitlich und vollständig sein. Damit einher geht das Vertrauen des Benutzers in die Zuverlässigkeit, die korrekte Funktion und die Wahrheit des Systems (oder einer Person). Vertrauen wird gewährt, ohne dass es Beweise oder Nachweise gibt. Wikipedia bezeichnet „Vertrauen" als „[…] die subjektive Überzeugung von der Richtigkeit, (oder auch das Gefühl für oder Glaube an die) Wahrheit von Handlungen, Einsichten und Aussagen bzw. der Redlichkeit von Personen". (Wikipedia, 2019)

Wie können nun Vertrauen und Integrität in verteilten Systemen sichergestellt werden und dies sogar in rein verteilten Systemen, in denen eine unbekannte Zahl von unbekannten Akteuren mit unbekannter Vertrauenswürdigkeit agiert, wo doch Vertrauen die Grundlage eines jeden Peer-to-Peer-Systems ist?

SATOSHI NAKAMOTO

BITCOIN

DISTRIBUTED LEDGER

„VERTRAUENS-MASCHINE“ BLOCKCHAIN

Im Jahr 2008 wurde zu dieser Frage unter dem Pseudonym Satoshi Nakamoto (vgl. Nakamoto, 2008) ein Dokument veröffentlicht, in dem ein elektronisches Bezahlsystem auf Basis der heute als Blockchain bekannten Technologie beschrieben wurde. Das Papier skizziert eine öffentliche Datenbank, die alle zehn Minuten Kopien ihrer selbst auf Hunderte oder sogar Tausende Computer verteilt und von diesen synchron gehalten wird. Ziel war es, eine öffentlich einsehbare, dezentrale und sichere Möglichkeit für eine digitale Währung zu schaffen, die der Autor „Bitcoin“ nannte. Kein Benutzer, keine Benutzergruppe, keine Administration, keine Bank und kein Staat sollten diese Währung regulieren oder manipulieren können. „Digitale Münzen“ (beziehungsweise in Analogie zur Teilbarkeit echten Geldes auch Teile davon) sind dabei eindeutig charakterisiert und werden, um zu vermeiden, dass Geld mehrfach ausgeben wird (vgl. Chohan, 2017), in ein verteiltes Hauptbuch (oder Kassenbuch), den sogenannten distributed ledger, geschrieben. Kryptografische Verfahren und spezielle Datenstrukturen sichern die Transaktionen und das Hauptbuch per Blockchain ab.[2] Der Economist betitelte 2015 diesen Ansatz als „Vertrauensmaschine“ (The Economist, 2015), die Blockchain sei „eine fantastische Kette des Vertrauens“, die „die Wirtschaft auf den Kopf stellen könne“, und dem Bitcoin wurde nachgesagt, eine Währung zu sein, die nur vom Vertrauen der Teilnehmer gedeckt sei. Dieses Vertrauen wurde vor allem durch die verwendeten Technologien und das zugrundeliegende Konzept geschaffen, das jede Transaktion unveränderlich, unfälschbar und öffentlich einsehbar macht. Inzwischen ist die Blockchain über die Bitcoin-Anwendung hinausgewachsen, da in den vergangenen Jahren deutlich wurde, dass im von Nakamoto beschriebenen verteilten Hauptbuch nicht nur Transaktionen, sondern auch Eigentumsnachweise, Dokumente, Zeugnisse, medizinische Daten oder Verträge unveränderlich abgelegt werden könnten.

2.3 Identität, Eigentum und Eigentumsverwaltung

ZUSAMMENFASSUNG

» **Die aus der IT-Sicherheit bekannten Konzepte zur Identifizierung, Authentisierung, Authentifizierung und Autorisierung sind Basisvoraussetzungen zum Nachweis einer Eigentümerschaft.**

DOKUMENTATION VON TRANSAKTIONEN

Dem von Nakamoto beschriebenen Anwendungsfall liegt ein (verteiltes) Hauptbuch („distributed ledger“) zur Dokumentation von Transaktionen zugrunde, in dem zusätzlich eine Zuordnung von Eigentümern zu Eigentumsobjekten erfolgt. Auch außerhalb der digitalen Welt sind Hauptbücher zu finden, in denen Identitäten oder Eigentumsnachweise verwaltet werden, häufig durch vertrauenswürdige Entitäten oder sogar durch ein staatlich reguliertes Hauptbuch dokumentiert. Diese Hauptbücher können teilweise öffentlich eingesehen werden, um im Streitfall Eigentumsüberprüfungen vornehmen zu können. Bekannte Beispiele sind Grundbücher, amtliche Dokumente wie Personalausweise oder Führerscheine, aber auch Bankkonten und andere Register zur Verwaltung von Heirats- oder Geburtsurkunden. An diesen Beispielen wird erkenntlich, dass es zwei Arten gibt, Eigentum nachzuweisen. Zum einen erfolgt der Nachweis über die Existenz eines gültigen Dokuments, also

Eigentums, welches den Ist-Zustand beschreibt, zum anderen über den Nachweis, per historischer Abfolge von Eigentumsübergängen in den Besitz einer Sache gekommen zu sein (zum Beispiel kann der Nachweis, im rechtmäßigen Besitz eines Autos zu sein, über eine lückenlose Kette von Kaufverträgen erfolgen oder über den Nachweis des Besitzes des Fahrzeugbriefs).

EIGENTUMSNACHWEISE PER ÖFFENTLICHEM HAUPTBUCH

Ein Eigentumsnachweis kann vor allem dann leicht erfolgen, wenn das Hauptbuch öffentlich einsehbar ist (also das Lesen öffentlich möglich ist). Eigentumsübertragungen dürfen dagegen nur durch die rechtmäßigen Eigentümer und der dazugehörige Eintrag im Hauptbuch (das Schreiben) nur durch eine entsprechend vertrauenswürdige Entität (die ggf. auch der Eigentümer sein kann) erfolgen.

KONSENS IN VERTEILTEN SYSTEMEN

Das Ziel besteht nun darin, das Eigentum auf nachvollziehbare Weise zu dokumentieren und so darzustellen, dass über die Dokumentation eine eindeutige und vertrauenswürdige Zuordnung des Eigentums zum Eigentümer erfolgen kann und das Hauptbuch die tatsächlichen Eigentumsverhältnisse widerspiegelt. Zum einen ist hierfür die Integrität des Hauptbuches fundamental. Wird das zentrale Hauptbuch gelöscht, beschädigt oder bewusst verändert, ist das Register für Eigentumsnachweise nicht mehr vertrauenswürdig. Um dies zu vermeiden, können Kopien mehrerer Hauptbücher parallel geführt werden, sodass beim Abklären von Eigentumsverhältnissen das als wahr angesehen wird, was in den meisten Hauptbüchern dokumentiert ist. Ein rein verteiltes Peer-to-Peer-System könnte auf diese Weise über die Mehrheit der Aussagen den Konsens eines Eigentumszustandes schaffen („Wahr ist, was die meisten sagen“).

Außer den Teilnehmern müssen auch Eigentum oder Transaktionen (als Eigentumsübergänge) eindeutig identifiziert werden können. In der IT-Sicherheit kennt man hierzu grundlegende Sicherheitskonzepte, die sich in einer Kette ergänzen und mitunter einander bedingen:

- Identifizierung;
- Authentisierung;
- Authentifizierung;
- Autorisierung.

IDENTIFIZIERUNG & AUTHENTISIERUNG

Die *Identifizierung* ist zunächst einmal nur die Behauptung von jemandem, eine bestimmte Person (oder ein Vorgang) zu sein, beispielsweise die Nennung eines Namens. Die Authentisierung stellt den Nachweis der Person dar, der belegt, dass die Person jene ist, die sie zu sein behauptet. Eine Identität ist der eindeutige Identifikator für eine Person, eine Organisation, eine Ressource oder eine Dienstleistung. Der Identifikator umfasst eindeutig kennzeichnende Merkmale. Der Nachweis, der die Identität bestätigt, kann zum Beispiel ein Personalausweis (Identifizierungsgegenstand), ein biometrisches Merkmal (Identifizierungsobjekt) oder eine geheime Information, die nur diese Person kennt (Passwort), sein. Die Identifizierung und die Authentisierung stellen den ersten Schritt zur Prüfung einer Identität dar.

AUTHENTIFIZIERUNG & AUTORISIERUNG

Im Rahmen der *Authentifizierung* wird die behauptete Authentisierung geprüft und die Identität einer Person bestätigt. Bei der Autorisierung werden dieser Person Rechte eingeräumt, die mit ihrer Identität verbunden sind.

Setzt man nun die Identität, das Eigentum und die Eigentumsübertragung zueinander in Relation, kann diese Kette folgendermaßen aufgebaut werden: Eine Person behauptet, Eigentümer eines Objekts zu sein (Identifizierung). Diese Person weist nach, dass sie tatsächlich diese Person ist (Authentisierung). Nach der Überprüfung (Authentifizierung) erfolgt die Autorisierung (die Einleitung einer Eigentumsübertragung). Für das

Eigentum gilt parallel ein vergleichbarer Vorgang. Es wird behauptet, dass dieses Eigentum und eine Zuordnung zwischen Objekt und Eigentümer existieren (Identifizierung und Authentisierung). Nachdem diese Zuordnung belegt ist (Authentifizierung), kann die Eigentumsübertragung in Form einer Transaktion erfolgen (Autorisierung).

2.4 Hash-Funktionen

ZUSAMMENFASSUNG

» **Kryptografische Hash-Funktionen haben bei der Blockchain eine hohe praktische Relevanz. Sie dienen als digitaler Fingerabdruck dem Nachweis einer Eigentümerschaft, dem effizienten Vergleich und Finden von Daten, dem Erkennen von Veränderungen, der Speicherung und dem Verweis von (Transaktions-)Daten auf veränderungsempfindliche Weise und dem Erzeugen von rechenintensiven, teuren Aufgaben zum Schutz vor Manipulationen und dem Erhalt der Integrität.**

↖ HASH-FUNKTIONEN

> „Technisch gesehen ist eine Blockchain eine dezentrale, auf vielen Computern verteilte Datenbank, mit der Aufzeichnungen von Transaktionen hinterlegt werden, die für jeden Teilnehmer dieser Blockchain einsehbar sind. Die Computer, die an einer Blockchain teilnehmen, sind über das Internet vernetzt und bilden damit ein Blockchain-Netzwerk. In jeden neuen Datensatz (‚block') wird eine kryptografische Prüfsumme (Hashwert) der bisherigen Kette (‚chain') von Datensätzen geschrieben, sodass eine Manipulation der Daten durch einzelne Teilnehmer im Prinzip unmöglich ist." (VDI Technologiezentrum, 2018, S. 2)

Hash-Werte werden von besonderen mathematischen Funktionen, den sogenannten Hash-Funktionen, berechnet, die beliebige Daten ungeachtet ihrer Länge (und Größe der Eingabemenge) auf eine Zahl fester Länge (in der Regel nicht-injektiv, vgl. Mathepedia, 2019) abbilden. Für die Blockchain sind Hash-Funktionen ein elementares und an vielen Stellen eingesetztes Werkzeug, weshalb in diesem Kapitel vertieft auf die Funktionsweise und Eigenschaften von Hash-Funktionen eingegangen werden soll.

Ein sehr einfaches Beispiel für eine Hash-Funktion ist die Bildung einer Quersumme, aber auch die Abbildung eines beliebigen Namens auf den Anfangsbuchstaben des Nachnamens ist vom Prinzip her eine Hash-Funktion.

TABELLE 1: MAPPING AUF DEN ANFANGSBUCHSTABEN DES NACHNAMENS

MAX MUSTERMANN	→	M
ALEXA SCHMIDT	→	S
BERTA SONNENSCHEIN	→	S

Quelle: Eigene Darstellung

Bereits an diesem einfachen Beispiel lassen sich Eigenschaften dieser speziellen Funktionen erkennen. Die Berechnung stellt eine schnelle und deterministische Einwegfunktion auf einen immer gleich langen Ausgabewert dar (hier der Länge 1). Im obigen Beispiel erfolgt zudem eine sogenannte Kollision, das heißt, zwei unterschiedliche Eingabewerte werden auf den gleichen Hash-Wert (Schlüssel) abgebildet, ein zur eindeutigen Identifizierung von Elementen unerwünschter Vorgang. In der Realität werden in bestimmten Anwendungskontexten ausschließlich Hash-Funktionen eingesetzt, bei denen die Wahrscheinlichkeit einer Kollision extrem niedrig ist.

KRYPTOGRAFISCHE HASH-FUNKTIONEN

Einen wichtigen Spezialfall von Hash-Funktionen stellen daher kryptografische Hash-Funktionen[3] dar, die sich durch folgende erweiterte Eigenschaften auszeichnen, die in der Folge detailliert erläutert werden:

- schnelle Abbildung beliebiger Daten auf Schlüssel fester Länge;
- Einwegfunktionen;
- deterministisch;
- pseudozufällig;
- kollisionssicher.

Eine Hash-Funktion ist also in der Lage, aus beliebig langen Eingabedaten sehr schnell Hash-Werte fester Länge zu berechnen. So werden von der weit verbreiteten kryptografischen Hash-Funktion MD5 (vgl. Rivest, 1992)[4] folgende Werte mit gleicher Länge berechnet:

TABELLE 2: ABBILDUNG VERSCHIEDEN LANGER EINGABEWERTE AUF AUSGABEN KONSTANTER LÄNGE

EINGABEWERT	HASH-WERT (MD5)
HAUS	ebacf61946ee81f386960ad2a09a147e
DIES HAUS IST MEIN UND DOCH NICHT MEIN. DER NACH MIR KOMMT, KANN'S AUCH NUR LEIH'N ...	6908359b3e91edbecb5cd4e3efe3461b

Quelle: Eigene Darstellung

EINWEGFUNKTIONEN

Einwegfunktionen sind in der Informatik mathematische Funktionen, die komplexitätstheoretisch leicht zu berechnen sind, wodurch eine Berechnung in Polynomialzeit möglich ist, die aber schwer umzukehren ist, das heißt, für die Umkehrfunktion existiert kein Algorithmus mit polynomialer Laufzeit (vgl. Sedgewick/Wayne, 2014). Ein bekanntes Beispiel aus der Praxis (für eine Einwegfunktion) ist die Herausforderung bei der Primfaktorzerlegung (vgl. Learn Cryptography, 2019), von der man annimmt, dass sie ein schwieriges Problem in exponentieller Größenordnung darstellt, wohingegen die Multiplikation von zwei großen Primzahlen eine leichte Aufgabe ist. Entsprechend lässt sich der MD5-Hash-Wert einer beliebigen Eingabe schnell berechnen, aber ein bestehender Hash-Wert kann aufgrund der Pseudozufälligkeit nicht mehr (beziehungsweise nur mit unverhältnismäßig großem Aufwand) in seinen Ursprungstext zurückverwandelt werden.

EXKURS: FINGERABDRÜCKE

Fingerabdrücke (beziehungsweise die Abbilder der sogenannten Papillarlinien) sind ein eindeutiges Unterscheidungsmerkmal beim Menschen. Sie werden in der Kriminalistik oder bei biometrischen Zugangssystemen zur Identifizierung von Personen eingesetzt. Der Fingerabdruck hängt nicht allein von den Erbanlagen des Einzelnen ab, sondern auch von zahlreichen Umgebungsfaktoren.

Die Besonderheit hierbei ist, dass bisher keine zwei Menschen mit einem gleichen Fingerabdruck bekannt sind, sodass man von der Einzigartigkeit des Fingerabdrucks als Unterscheidungsmerkmal ausgeht. Das digitale Gegenstück zum Fingerabdruck sind in der Informationstechnik die sogenannten Hashes (oder Hash-Werte).

↖ **DETERMINISTISCHE FUNKTIONEN**

Deterministisch bedeutet, dass die Hash-Funktion für die gleichen Eingabewerte immer wieder und reproduzierbar die gleichen Hash-Werte berechnet. Unterschiede im Hash-Wert dürfen bei Verwendung der gleichen Hash-Funktion ausschließlich über Unterschiede in der Eingabemenge zustande kommen.

↖ **PSEUDOZUFÄLLIGKEIT**

Pseudozufällig heißt, dass der berechnete Hash-Wert sich auf nicht vorhersehbare Weise verändert, sobald die Eingabemenge auch nur minimal verändert wird. Damit sollen geringste Unterschiede in der Eingabe zu großen Veränderungen in der Ausgabe führen, wodurch eine Manipulation sofort offensichtlich wird. Tabelle 3 zeigt, wie kleinste Änderungen den Hash-Wert vollständig verändern.

TABELLE 3: AUSWIRKUNGEN VON VERÄNDERUNGEN AUF DEN BERECHNETEN HASH-WERT

EINGABEWERT	HASH-WERT (MD5)
HAUS	ebacf61946ee81f386960ad2a09a147e
LAUS	c3694b483eed355a49954b09f345df09
LAUT	fdf7e0ae1f79bade748514ddc4607b8f

Quelle: Eigene Darstellung

↖ **KOLLISIONSRESISTENZ**

Die *Kollisionssicherheit* (oder auch Kollisionsresistenz) ist eine weitere wichtige Eigenschaft kryptografischer Hash-Funktionen. Bei idealen Hash-Funktionen ist die Wahrscheinlichkeit, für verschiedene Eingabemengen denselben Hash-Wert zu berechnen, sehr gering. Das bedeutet, dass es nicht effizient möglich ist, zwei unterschiedliche Nachrichten mit demselben Hash-Wert zu finden. Wird für unterschiedliche Eingaben der gleiche Hash-Wert errechnet, spricht man von einer Kollision, vergleichbar mit dem Finden zweier Menschen mit identischem Fingerabdruck. Um die Einzigartigkeit digitaler Fingerabdrücke/Signaturen zu gewährleisten, ist somit eine kryptografische Hash-Funktion notwendig. Während die bereits eingeführte Kryptowährung Bitcoin auf ihrer Blockchain die Hash-Funktion SHA-256

(Secure Hash Algorithm der SHA-2-Familie, vgl. Federal Information Processing Standards Publication, 2002) verwendet, nutzen andere Implementierungen Funktionen wie SHA-3 (vgl. Equibit Group, 2017) oder RIPEMD160 (vgl. Github, 2019).

SHA-256

WEITERE VERWENDUNGSMÖGLICHKEITEN VON HASH-FUNKTIONEN

Eine weitere Besonderheit stellt die kombinierte Anwendung von Hash-Funktionen dar. Verschiedene Daten können nicht nur einzeln, sondern auch deren Hash-Werte können sequenziell oder hierarchisch in einen neuen kombinierten Hash-Wert überführt werden. So können die Datensätze einer Datenbank für sich mit Hash-Werten versehen werden, aber auch die Hash-Werte ihrerseits können kombiniert mit einem erneuten Aufruf der Hash-Funktion zu einem neuen Hash gleicher Länge abgebildet werden. Es entsteht immer wieder ein eindeutiger, deterministischer, pseudozufälliger und kollisionsresistenter Ausgabewert fester Länge.

SCHNELLER VERGLEICH VON INHALTEN

Die Forderung und das Beispiel von Pseudozufälligkeit und Kollisionssicherheit haben gezeigt, dass mit Hash-Werten vor allem eines sehr gut geleistet werden kann: Inhalte von (nahezu beliebig langen) Daten können schnell und einfach miteinander verglichen werden, ohne dass zeichen- beziehungsweise bitweise die Dokumente/Informationen einander gegenübergestellt werden müssen. Sind die Hash-Werte verschieden, so ist mindestens ein Zeichen in einem der Vergleichsdokumente unterschiedlich. Das Erkennen von Veränderungen durch Manipulation ist ein grundlegender Anwendungsfall der Hash-Funktionen. Bei der Blockchain findet dies unter anderem Anwendung bei der manipulationssicheren Speicherung von Transaktionsdaten (die über ihren digitalen Fingerabdruck per Hash-Wert identifiziert werden können) in Form von sogenannten Hash-Referenzen. Dabei wird für die hinterlegten Daten ein Hash-Wert berechnet und als Verweis (Referenz) verwendet. Abbildung 4 zeigt, wie Daten mit Hash-Referenzen in einer Baumstruktur organisiert werden können. Dieser sogenannte Merkle Tree (oder auch Hash-Baum), benannt nach dem Informatiker Ralph Merkle (vgl. Merkle, 1979), zeichnet sich dadurch aus, dass jede geringfügige Veränderung, egal an welcher Stelle, sofort und leicht nachvollziehbar an der Wurzel des Baumes zu überprüfen ist. Wird eine einzelne Referenz in einem Ast des Baumes verändert, so führt diese Veränderung zu Inkonsistenzen, die an der Wurzel des Baumes überprüft werden können.

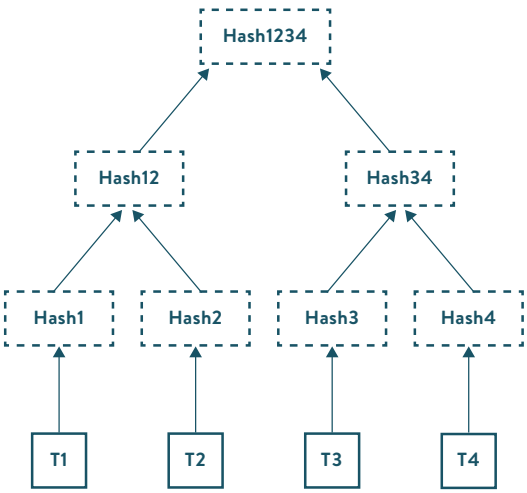
HASH-REFERENZEN

Hierzu wird für jede einzelne Transaktion ein Hash-Wert berechnet und dieser dann pyramidenförmig zur Wurzel weitergerechnet, bis am Ende nur noch der Root-Hash des vollständigen Baumes übrig bleibt. Ein Merkle-Baum ist also eine Datenstruktur, die durch wiederholtes Hashen, zunächst paarweise der Transaktionen und anschließend von Paaren von Hash-Werten, bis zur Wurzel entsteht. Anhand dieser Hash-Wurzel kann zudem jede Transaktion im Block auf ihre Existenz hin überprüft werden.

MERKLE TREE (HASH-BAUM)

ABBILDUNG 4: EIN BINÄRER HASH-BAUM MIT SUKZESSIV KOMBINIERTER HASH-WURZEL

Der Merkle Tree zeichnet sich dadurch aus, dass jede geringfügige Veränderung, egal an welcher Stelle, sofort und leicht nachvollziehbar an der Wurzel des Baumes zu überprüfen ist.



Quelle: Eigene Darstellung

Abschnitt 2.6 wird im Detail zeigen, wie Transaktionsdaten mithilfe von Hash-Werten und Referenzen manipulationssicher gespeichert und gefunden werden können. Es gibt jedoch noch eine weitere Besonderheit bei Hash-Funktionen, die bei der Blockchain eine hohe praktische Relevanz hat. In der Einleitung wurde bereits erwähnt (und wird in Abschnitt 2.9 weiter vertieft), dass die Bitcoin-Blockchain einen Strombedarf vergleichbar mit dem Stromverbrauch ganzer Staaten (vgl. Digiconomist, 2019) verursacht. Der Grund hierfür liegt in den beschriebenen Eigenschaften der Hash-Funktionen, denn diese werden bei der (Bitcoin-)Blockchain dergestalt eingesetzt, dass Manipulationen von Daten (im Merkle Tree und organisiert als Kette von Blöcken) schlicht unwirtschaftlich werden. Abschnitt 2.8 wird dies detailliert am Beispiel der Bitcoin-Blockchain illustrieren. Die Pseudozufälligkeit der Einwegfunktion kann dazu genutzt werden, eine Aufgabe zu formulieren, deren Lösung nur durch den Einsatz reiner Rechenleistung erreicht werden kann. Die sogenannten Hash-Puzzles (oder auch Computational Puzzles beziehungsweise Proofs of Work) sind Berechnungsaufgaben zum Finden eines (Ziel-)Hash-Wertes mit vordefinierten Eigenschaften, die nur über Durchprobieren (Trial and Error) von Eingabekombinationen gelöst werden können. Es existiert kein Algorithmus, der die Richtung einer Hash-Funktion umzukehren vermag, um auf diese Weise das Hash-Puzzle effizient lösen zu können. Beim Hash-Puzzle der Blockchain werden einige Datenfelder der Blockchain (Abschnitt 2.6 beschreibt dies im Detail) mit einem variablen Informationsteil („Nonce“[5]) zu einem neuen Hash-Wert verknüpft, der über eine zusätzliche Bedingung bestimmte Merkmale erfüllen muss. Das Rätsel besteht nun darin, den variablen Teil so lange zu verändern, bis der berechnete Gesamt-Hash-Wert dieser zusätzlichen Bedingung entspricht. Die Bedingung zur Beschreibung der geforderten Hash-Wert-Eigenschaft wird häufig als Schwierigkeitsgrad (oder „Difficulty“) beschrieben, da mit dem Umfang

↖ **SCHWIERIGKEITSGRAD EINES HASH-PUZZLES**

der Ausgestaltung der Bedingung die Anzahl der Versuche, um eine Lösung zu finden, gesteuert werden kann. So könnte eine Bedingung beispielsweise lauten: „Finde für die Verknüpfung von Datenfeld und Nonce einen Hash-Wert, der mit einer (zwei, drei oder noch mehr) führenden Null beginnt." Tabelle 4 zeigt ein solches Schema.

TABELLE 4: FINDEN EINES NONCE, DER ANGEHÄNGT AN EINE NACHRICHT EINEN HASH-WERT MIT ZUM BEISPIEL FÜNF FÜHRENDEN NULLEN ERZEUGT

NACHRICHT/DATEN	NONCE*	MD5-HASH
DAS, WOBEI UNSERE BERECHNUNGEN VERSAGEN, NENNEN WIR ZUFALL.	1	a91c28c8bb3c50c084bfdbc86be8c1a3
DAS, WOBEI UNSERE BERECHNUNGEN VERSAGEN, NENNEN WIR ZUFALL.	2	990dd6051c462dece247496934b301bb
DAS, WOBEI UNSERE BERECHNUNGEN VERSAGEN, NENNEN WIR ZUFALL.	30	06656dff15ab8cebb1b81fcb0a808404
DAS, WOBEI UNSERE BERECHNUNGEN VERSAGEN, NENNEN WIR ZUFALL.	1821	00cbef06855cebe24a051116ecd52c80
DAS, WOBEI UNSERE BERECHNUNGEN VERSAGEN, NENNEN WIR ZUFALL.	5530	000b3419067b62eb5cab493e16175671
DAS, WOBEI UNSERE BERECHNUNGEN VERSAGEN, NENNEN WIR ZUFALL.	23805	0000f8c06a70e910053115e2d73954c5
DAS, WOBEI UNSERE BERECHNUNGEN VERSAGEN, NENNEN WIR ZUFALL.	341197	000007377d98e6ff1fdd5b7cf5211182

* In diesem Beispiel werden als Nonce aufsteigende Zahlen verwendet.
Quelle: Eigene Darstellung

Das Lösen dieser Aufgabe kostet aufgrund der Pseudozufälligkeit und der damit verbundenen Notwendigkeit, Lösungen durch Ausprobieren zu finden, viel Rechenleistung und damit Zeit und Energie.[6] Bei der Blockchain werden solche Hash-Puzzles daher als Proof of Work, also als Arbeitsnachweis für die gefundene Lösung bezeichnet. Das Überprüfen der Korrektheit einer Lösung wiederum kann aufgrund der bisher beschriebenen Eigenschaften der Hash-Funktion schnell geschehen.

↖ PROOF OF WORK

In Abschnitt 2.6 wird gezeigt, wie die Blockchain als Datenspeicher angelegt ist, Abschnitt 2.9 stellt dar, wie das Verändern der Schwierigkeit dazu genutzt wird, Manipulationsversuche auf der Blockchain unrentabel zu machen, unabhängig davon, wie viel Rechenleistung im Verbund des verteilten Systems zur Verfügung steht.

2.5 Asymmetrische Kryptografie als Grundlage der Blockchain

ZUSAMMENFASSUNG

» **Durch die Kombination asymmetrischer Kryptografie und digitaler Signaturen von Benutzerkonten und Transaktionen, wie sie in der Blockchain kodiert werden, kann sicher nachgewiesen beziehungsweise überprüft werden, dass eine Transaktion von einem Benutzer autorisiert wurde. Eigentum kann auf diese Weise nachvollziehbar zurückverfolgt werden, Kapitel 1.3 hat dies angekündigt, indem der Nachweis von Eigentum auch über die historische (und vollständige) Abfolge von Eigentumsübergängen erfolgen kann.**

Üblicherweise kann eine Eigentumsübertragung nur durch den rechtmäßigen Eigentümer erfolgen, weswegen eine eindeutige Identifizierung und in der Folge Autorisierung als Nachweis notwendig ist. In einem öffentlich zugänglichen verteilten System wie der (Bitcoin-)Blockchain kann jedermann teilnehmen und Transaktionsdaten übermitteln, doch die Übertragung von Eigentum ist exklusiv dem Eigentümer vorbehalten. Die Kryptografie, ursprünglich die Wissenschaft der Verschlüsselung von Informationen, dient im Kontext der Informationssicherheit dem Schutz von Daten vor Zugriff durch unberechtigte Dritte. Im Falle der Blockchain wird mithilfe kryptografischer Methoden sichergestellt, dass nur der Eigentümer in der Lage ist, eine Eigentumsübertragung vorzunehmen.

KRYPTOGRAFIE, DIE WISSENSCHAFT DER VERSCHLÜSSELUNG VON INFORMATIONEN

Unterschieden wird zwischen symmetrischen und asymmetrischen Kryptoverfahren. Bei symmetrischen Kryptoverfahren (Secret Key) wird zum Ver- und Entschlüsseln der gleiche Sicherheitsschlüssel (zum Beispiel ein Passwort) verwendet. In der Regel sind diese Verfahren auf ressourcenschonende Umgebungen ausgelegt, da sie sich durch geringe Hardwareanforderungen, niedrigen Energieverbrauch und einfache Implementierung auszeichnen. Sie bieten zudem bei ausreichend langen Schlüsseln eine hohe Sicherheit. Zu den bekanntesten symmetrischen Verschlüsselungsverfahren zählt der Advanced Encryption Standard (AES), der im Jahr 2000 vom National Institute of Standards and Technology (NIST) als Standard für symmetrische Verschlüsselung bekanntgegeben wurde (vgl. National Institute of Standards and Technology, 2019). Er findet heute noch Anwendung beispielsweise bei der Verschlüsselung von WLAN-Netzwerken per WPA2 (vgl. Institute of Electrical and Electronics Engineers, 2019).

SYMMETRISCHE KRYPTOVERFAHREN

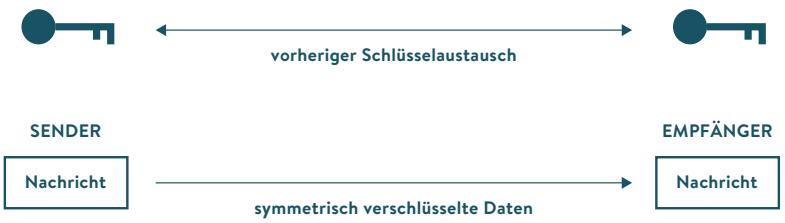
Ein großer Nachteil symmetrischer Verfahren liegt in der Verwendung desselben Schlüssels zur Ver- und Entschlüsselung, das heißt, außer den verschlüsselten Daten muss zudem auch der Schlüssel an den Kommunikationspartner über einen sicheren, üblicherweise anderen Kanal übermittelt werden, gegebenenfalls per Telefon oder physisch per Boten. In der Praxis hat sich diese Vorgehensweise verständlicherweise zunehmend als nicht praktikabel erwiesen.

Hier setzen die asymmetrischen Kryptoverfahren an (Public Key), bei der zwei einander ergänzende Schlüssel als Schlüsselpaar zum Einsatz kommen. Ein Schlüssel wird zum Ver- und der andere zum Entschlüsseln verwendet. Damit existiert ein öffentlicher Schlüssel (Public Key) des Empfängers, der beim Versender zum Verschlüsseln eingesetzt wird. Der andere Schlüssel (Private Key) dient dem Empfänger zum Entschlüsseln der Nachricht.

ASYMMETRISCHE KRYPTOVERFAHREN

ABBILDUNG 5: SYMMETRISCHES UND ASYMMETRISCHES VERSCHLÜSSELUNGS-VERFAHREN

Symmetrisches Verschlüsselungsverfahren: Gleicher Schlüssel beim Ver- und Entschlüsseln



Asymmetrisches Verschlüsselungsverfahren: Der öffentliche Schlüssel (blau) wird zum Verschlüsseln verwendet, der private, geheime Schlüssel (rot) beim Entschlüsseln durch den Empfänger.

Quelle: Eigene Darstellung

Etwas genauer kann der Ablauf des asymmetrischen Verschlüsselungsverfahrens folgendermaßen umrissen werden:

- Der Empfänger generiert ein Schlüsselpaar, bestehend aus dem privaten Schlüssel (Private Key) und dem öffentlichen Schlüssel (Public Key).
- Der private Schlüssel ist geheim und verbleibt beim Empfänger. Mit diesem Schlüssel können Nachrichten entschlüsselt werden.
- Der öffentliche Schlüssel wird publik gemacht und dient dem Versender (oder den Versendern) zum Verschlüsseln einer Nachricht.

↖ **PUBLIC-KEY-KRYPTOGRAFIE**

Aufgrund der Eigenschaften der bei der Generierung der Schlüssel verwendeten Einwegfunktionen kann leicht ein zusammengehöriges Schlüsselpaar berechnet werden, doch die Gegenrichtung ist komplexitätstheoretisch schwer. Allein aus der Kenntnis des Public Keys können keine Rückschlüsse auf den Private Key gezogen werden. Dementsprechend wird die asymmetrische Kryptografie auch als Public-Private-Key-Kryptografie (oder auch Public-Key-Kryptografie) bezeichnet.

Zu den Nachteilen asymmetrischer Verschlüsselungsverfahren zählt unter anderem der erhöhte Aufwand bei mehreren Empfängern. Da die Verschlüsselung mit dem individuellen Public Key eines jeden Empfängers erfolgt, muss die Nachricht auch für jeden Empfänger einzeln verschlüsselt werden. Zudem kann es zu einem (Schlüssel-) Verteilungsproblem über einen sogenannten „Man-in-the-Middle"-Angriff kommen. Hierbei positioniert sich ein Mittelsmann in der Kommunikation zweier Personen

und täuscht seinen eigenen Public Key als den des Empfängers vor. Er entschlüsselt mit seinem eigenen Private Key die Nachricht des Versenders, verschlüsselt diese anschließend mit dem Public Key des eigentlichen Empfängers und schickt die Nachricht weiter. Im schlimmsten Fall merken die Kommunikationspartner nicht, dass die Nachricht tatsächlich gelesen wurde. Um ein solches Szenario zu verhindern, muss gewährleistet sein, dass der verwendete Public Key authentisch, also dem gewünschten Empfänger zugehörig ist. Hierzu können Zertifikationsstellen dienen, bei denen Public Keys hinterlegt und deren Authentizität geprüft werden kann. Tatsächlich existiert für den beschriebenen Anwendungsfall bereits eine Sicherheitsinfrastruktur, die sogenannte Public Key Infrastructure (PKI). Das Bundesamt für Sicherheit in der Informationstechnik schreibt hierzu:

PUBLIC KEY INFRASTRUCTURE (PKI)

> „Besonderes Merkmal der Public Key Infrastructure (PKI) ist die Zertifizierungsstelle. Das ist eine allgemein anerkannte Stelle, deren Aufgabe es ist, die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel, siehe Asymmetrische Verschlüsselung) natürlichen Personen fest zuzuordnen und dies den Benutzern mittels ‚Zertifikaten' zu bestätigen." (Bundesamt für Sicherheit in der Informationstechnik, 2019)

Die bekanntesten Public-Key-Algorithmen sind RSA (benannt nach den Mathematikern Rivest, Shamir und Adleman) oder der später eingesetzte Algorithmus Elgamal des Kryptologen Taher Elgamal (vgl. Beutelspacher/Neumann/Schwarzpaul, 2005).

Die Blockchain nutzt die asymmetrische Kryptografie in zwei Anwendungsfällen. Zum einen werden in der Blockchain Nutzer(-konten) identifiziert, um gemäß Abschnitt 2.3 die Zuordnung zwischen Eigentümer und Eigentum(-sobjekt) herzustellen und damit auch den Transfer von Eigentum zwischen den Nutzern vorzubereiten. Nutzerkonten sind auf der Blockchain als Adressen in Form kryptografischer Hash-Werte kodiert, die über einen öffentlichen kryptografischen Schlüssel repräsentiert sind. Das Standardformat für Bitcoin-Adressen ist „P2PKH" („Pay To Public Key Hash") (vgl. Antonopoulos, 2017). Dieser durch Hash-Funktionen berechnete Schlüssel (Hash-Wert) wird durch 26 bis 35 alphanumerische Zeichen, beginnend mit 1 oder 3 (beispielsweise 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2), dargestellt und ist der öffentliche Schlüssel für den Empfang für Bitcoin-Zahlungen. Zum anderen wird der private Schlüssel vom Nutzer verwendet, um eine Transaktion zu autorisieren und um auf sein Konto beziehungsweise seine Daten Zugriff zu erhalten. Dieser Schlüssel dient als exklusiver Nachweis (denn nur der Eigentümer kennt den privaten Schlüssel), dass der Eigentümer die Transaktion von seinem Konto aus rechtmäßig initiiert hat. Die anderen Teilnehmer des Netzwerks können mit dem öffentlichen Schlüssel prüfen, ob das in der Transaktion verwendete Konto mit dem Konto, von dem aus das Eigentum übertragen werden soll, identisch ist.

BITCOIN-ADRESSEN

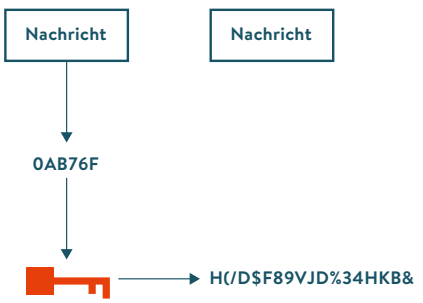
Die digitale Analogie zur eigenhändigen Unterschrift unter einem Dokument als Legitimationsprüfung (zum Beispiel bei einer Überweisung, einem Vertrag oder einer anderen Art der Eigentumsübertragung) ist die digitale Signatur. Sie verwendet eine Kombination aus kryptografischen Hash-Funktionen und dem Prinzip der asymmetrischen Kryptografie. Eine digitale Nachricht wird dabei mit dem geheimen Schlüssel des Versenders kombiniert, wodurch eine Signatur entsteht. Der Empfänger kann dann mit dem öffentlichen Schlüssel die nicht abstreitbare Urheberschaft (Identität und Autorisierung) und die Integrität der Nachricht (Korrektheit) prüfen.

DIGITALE SIGNATUR

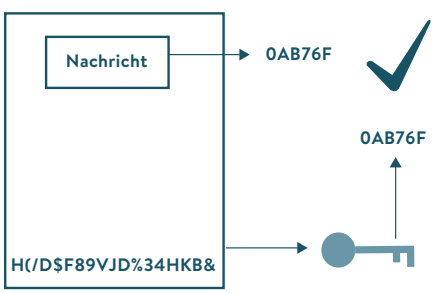
Die nachfolgenden Abbildungen zeigen schematisch, wie eine digitale Signatur zur Überprüfung einer Nachricht/Transaktion verwendet werden kann.

ABBILDUNG 6: FUNKTIONSWEISE EINER DIGITALEN SIGNATUR ZUR ÜBERPRÜFUNG EINER TRANSAKTION

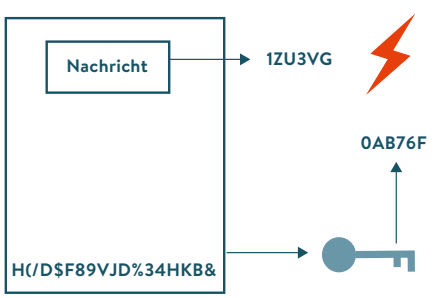
1) Der Hash-Wert einer Nachricht wird mit dem privaten Schlüssel des Versenders zu einer Signatur verschlüsselt.



2) Der Empfänger dekodiert die Signatur mit dem öffentlichen Schlüssel des Empfängers und prüft, ob der Hash-Wert der Nachricht identisch ist.



3) Stimmt der vom Empfänger berechnete Hashwert der Nachricht nicht mit dem des Versenders überein, so wurde die Nachricht in dieser Form nicht vom Versender autorisiert.



Quelle: Eigene Darstellung

2.6 Blockchain als Datenspeicher

ZUSAMMENFASSUNG

» **Die Blockchain-Datenstruktur besteht aus einer sequentiellen Anordnung von Elementen, die Blöcke genannt werden. Jeder dieser Blöcke besteht aus einem Header und einem Hash-Baum mit Daten, auf den im Header veränderungssensitiv (das heißt, Veränderungen können leicht erkannt werden) referenziert wird. Die Block-Header werden über einen Hash-Wert charakterisiert, der den kompletten Block, bestehend aus Header-Daten und Transaktionsdaten, umfasst und als Hash-Referenz für den nachfolgenden Block dient. Auf diese Weise verursachen bereits minimale Veränderungen an Teilen der Blockchain große Auswirkungen bei den Hash-Referenzen, sodass Verletzungen der Integrität schnell erkannt werden können.**

> „Technisch gesehen ist eine Blockchain eine dezentrale, auf vielen Computern verteilte Datenbank, mit der Aufzeichnungen von Transaktionen hinterlegt werden, die für jeden Teilnehmer dieser Blockchain einsehbar sind. Die Computer, die an einer Blockchain teilnehmen, sind über das Internet vernetzt und bilden damit ein Blockchain-Netzwerk. In jeden neuen Datensatz (‚block') wird eine kryptografische Prüfsumme (Hashwert) der bisherigen Kette (‚chain') von Datensätzen geschrieben, sodass eine Manipulation der Daten durch einzelne Teilnehmer im Prinzip unmöglich ist. Jeder neue Block wird durch ein dezentrales Konsensverfahren geschaffen und an die Blockchain angehängt, durch das die Reihenfolge der Datensätze in der Blockchain festgelegt wird." (VDI Technologiezentrum, 2018, S. 2)

↖ **VOLLSTÄNDIGE HISTORIE VON TRANSAKTIONEN**

Eine zentrale Aufgabe der Blockchain ist es, die vollständige Historie von Transaktionen sicher und transparent zu speichern, und zwar dergestalt, dass die Reihenfolge der Transaktionen erhalten bleibt und Veränderungen durch Manipulationen schnell erkannt werden können. Die grundlegenden Werkzeuge hierzu (Verteilte Systeme, Hashfunktionen, Merkle-Tree und asymmetrische Kryptographie und digitale Signaturen) wurden in den vorhergehenden Kapiteln bereits vorgestellt. In diesem Kapitel soll auf den Aufbau und die Struktur der Blockchain sowie die Anordnung der Transaktionen als „Kette von Blöcken" (Blockchain) eingegangen und die bekannten Werkzeuge sollen zu einem Gesamtbild zusammengefügt werden. Exemplarisch soll hier erneut die Bitcoin-Blockchain betrachtet werden, an der sich das Grundprinzip kryptografisch verketteter Datensätze gut nachvollziehen lässt.

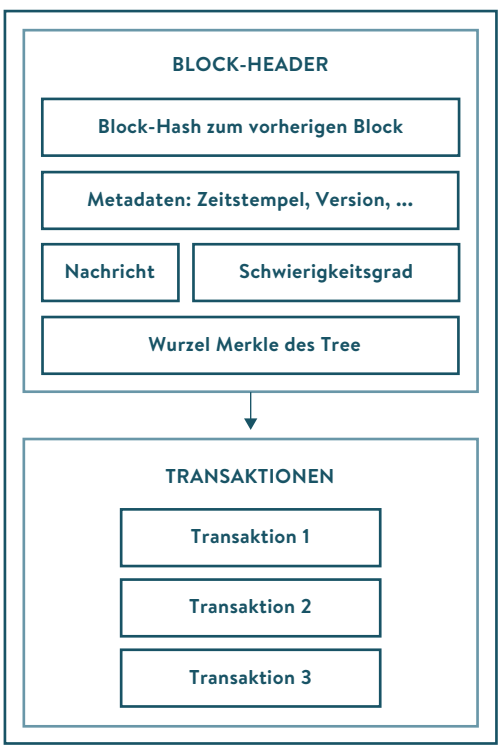
Als analoges Hilfsmittel lässt sich die dem Leser vorliegende Studie betrachten. Auf den Seiten der Studie sind Informationen in Form von Text zusammengestellt. Jede Seite ist mit einer Seitennummer versehen, die zwar über ein Inhaltsverzeichnis referenziert, aber vor allem durch die festgelegte und unveränderliche Anordnung der Seiten aufsteigend sortiert sind.

Würde eine Seite entfernt, so ließe sich das im Fehlen einer Seitennummer sofort erkennen. Die Studie ist also gegenüber dem Entfernen oder Hinzufügen von Seiten robust (vor allem in gedruckter Form). Auch gegen inhaltliche Veränderungen könnte die Studie abgesichert werden, indem auf jeder Seite der Hash-Wert über den Inhalt der jeweiligen Seite berechnet und auf der vorliegenden und nachfolgenden Seite vermerkt würde. Zusätzlich könnte auf dem Deckblatt der Studie ein Gesamt-Hash-Wert über alle Hash-Werte jeder Seite berechnet werden. So wären Reihenfolge

und Inhalte robust gesichert und nachträgliche Änderungen könnten durch die Überprüfung und Neuberechnung der Hash-Werte schnell erkannt werden. Mit einer weiteren minimalen, aber praktischen Transformation kann man sich der tatsächlichen Blockchain-Struktur noch weiter annähern. Würde man die Inhalte der Seiten herauslösen und nur die Daten verwalten, die zur Sicherung von Reihenfolge und Aufrechterhaltung der Integrität der Inhalte notwendig wären, könnten die Seiten der Studie sogar ausgelagert und per Hash-Referenz auf die jeweilige Seite verwiesen werden. Der ausgelagerte Inhalt wäre über den Hash-Wert der Seite nach wie vor unveränderlich gesichert. Diese Aufteilung von Inhalt (Transaktionen) und „Verwaltungsinformationen" ist auch in den Blöcken der Blockchain zu finden. Abbildung 7 zeigt schematisch, wie ein Block aufgebaut ist.

↖ AUFTEILUNG VON INHALT UND VERWALTUNGSINFORMATIONEN

ABBILDUNG 7: SCHEMATISCHER AUFBAU EINES BLOCKS EINER BLOCKCHAIN



Quelle: Eigene Darstellung

Während die Block-Kopfzeile (der sogenannte Header[7]) alle Informationen zur Verwaltung in sich trägt, wird der Inhaltsteil vom Header gesondert verwaltet und lediglich über eine Referenz verbunden. Beide Teile zusammen sind aber Bestandteil eines Blocks. Außerhalb des Headers werden die Transaktionen wie in Abschnitt 2.4 beschrieben über die veränderungssensitive Datenstruktur eines Merkle-Tree verwaltet. Die Wurzel des Merkle-Tree wird als Referenz im Header hinterlegt und anhand dieser Hash-Wurzel kann bereits über den Header geprüft werden, ob eine Transaktion im referenzierten Block enthalten ist. Diese Vorgehensweise hat in der Praxis große Vorteile, da die so entstandene Block-Kopfzeile um ein erhebliches

↖ BLOCKCHAIN-HEADER

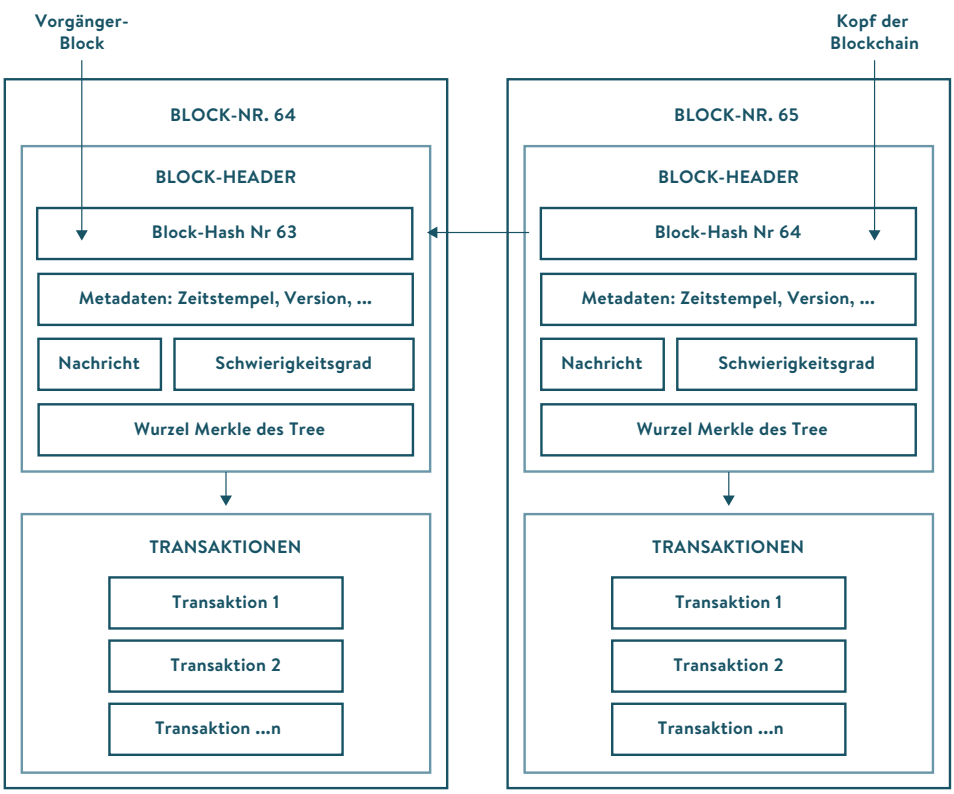
Maß kleiner ist als der ganze Block. Die weiteren Elemente des Headers sind ebenfalls aus den vorhergehenden Kapiteln bekannt.

METADATEN DES HEADERS

Außer dem Datenfeld für die Wurzel des Merkle Tree der im Block enthaltenen Transaktionen gibt es Felder für Zeitstempel, eine Hash-Referenz auf den Vorgänger-Block sowie weitere technische Metadaten wie zum Beispiel Versionsnummern und die beiden Felder Nonce und den Schwierigkeitsgrad des aktuellen Blocks. Über den Header des Blocks (und die darin enthaltene Referenz auf den Hash-Baum der Transaktionen) wird nun ein Gesamt-Block-Hash erzeugt, auf den dann im Folgeblock referenziert wird.[8] Abbildung 8 zeigt schematisch die lineare Verkettung von Blöcken und wie der eben beschriebene Block-Hash als Referenz auf den Vorgängerblock eingesetzt wird.

ABBILDUNG 8: VERKETTUNG DER BLÖCKE ÜBER DEN BLOCK-HASH DES VORGÄNGERBLOCKS

Der „Kopf" der Blockchain ist der jüngste Block, in den aktuelle Transaktionen eingefügt werden.



Quelle: Eigene Darstellung

BLOCKCHAIN-EXPLORER DER BITCOIN-BLOCKCHAIN

Wie ein solcher Block in natura aussieht, kann über den Blockchain-Explorer der Bitcoin-Blockchain eingesehen werden. Da Bitcoin eine öffentliche Blockchain ist, können dort Transaktionen und Blöcke in Echtzeit beobachtet werden.[9]

2.7 Einfügen und Überprüfen von Transaktionen

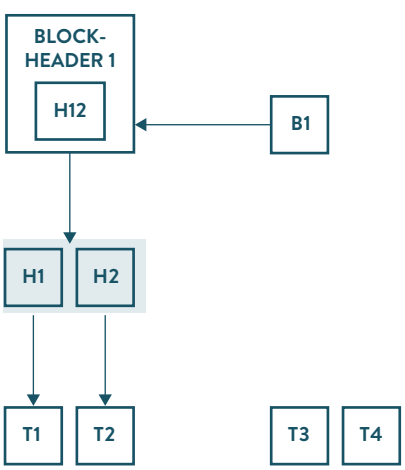
ZUSAMMENFASSUNG

» **Die Aufrechterhaltung der Integrität der Blockchain ist direkt verbunden mit der Korrektheit aller enthaltenen Hash-Referenzen. Wird nur eine dieser Referenzen ungültig, was leicht geprüft werden kann, verliert die komplette Blockchain ihre Gültigkeit. Hierdurch wird die Blockchain zu einer enorm änderungssensitiven Datenstruktur. Neue Einträge werden an den Kopf der Kette und damit an den aktuellen Block angehängt und der kumulierte Block-Hash-Wert für diesen dann berechnet. Sollten dennoch „im hinteren Teil" der Kette Änderungen erfolgen müssen, so ist es konzeptionell bedingt zwingend notwendig, die gesamte Blockchain-Datenstruktur vom Ort der Änderung bis zum Kopf (also dem aktuellen Block) vollständig neu zu berechnen.**

> „Jeder neue Block wird durch ein dezentrales Konsensverfahren geschaffen und an die Blockchain angehängt, durch das die Reihenfolge der Datensätze in der Blockchain festgelegt wird." (VDI Technologiezentrum, 2018, S. 2)

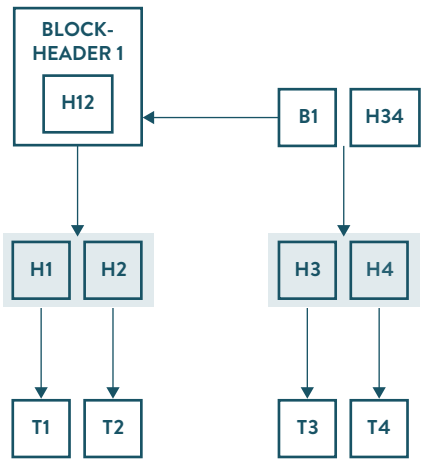
Beim Einfügen und Überprüfen von Transaktionen (Daten) in die Blockchain wird einmal mehr die Mächtigkeit von Hash-Referenzen deutlich. In Abbildung 9 ist schematisch eine Situation dargestellt, in der zwei Transaktionen T3 und T4 als neuer Block in eine Blockchain-Datenstruktur eingefügt werden sollen. Die Hash-Referenzen H1 und H2 sind als Referenzen der bisherigen Transaktionen T1 und T2 über die Referenz H12 Teil des Hash-Baumes (Merkle Trees) in diesem Block. Der Blockheader 1 beziehungsweise die Hash-Referenz B1 ist der Hash-Wert, wie er in Kapitel 1.6 konstruiert worden ist und als Referenz für einen neuen Block dient.

ABBILDUNG 9: ZWEI TRANSAKTIONEN T3 UND T4 SOLLEN AN EINE BLOCKCHAIN ANGEHÄNGT WERDEN



Quelle: Eigene Darstellung

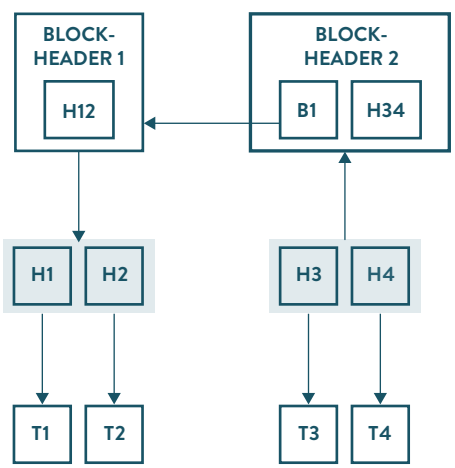
ABBILDUNG 10: DIE HASH-WURZEL H34 WIRD AUS DEN TRANSAKTIONEN T3 UND T4 ERSTELLT



Quelle: Eigene Darstellung

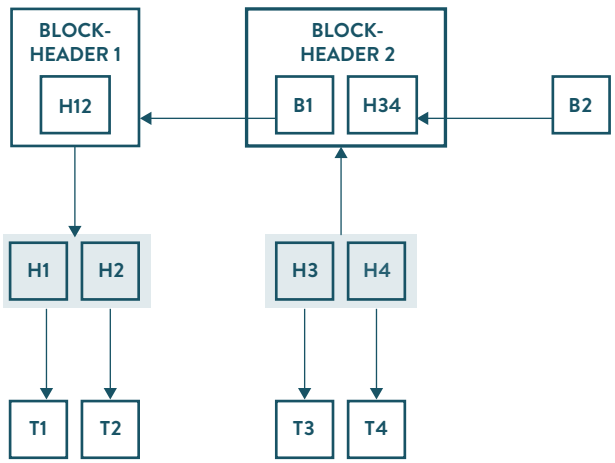
Abbildung 10 zeigt in einem ersten Schritt, wie für die Transaktionen T3 und T4 ein Merkle Tree erstellt worden ist und dieser über den Wurzel-Hash H34 repräsentiert wird. Im zweiten Schritt wird ein neuer Blockheader 2 erstellt, der den Wurzel-Hash H34 sowie die Hash-Referenz B1 des Vorgängerblocks berücksichtigt. Abbildung 11 zeigt diesen Schritt.

ABBILDUNG 11: BLOCKHEADER 2 DES NEUEN BLOCKS WIRD GENERIERT



Quelle: Eigene Darstellung

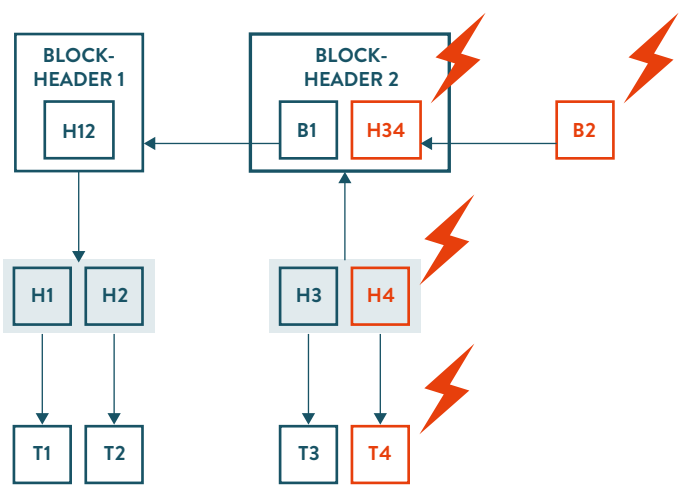
ABBILDUNG 12: B2 IST NEUER KOPF DER AKTUALISIERTEN BLOCKCHAIN



Quelle: Eigene Darstellung

Im dritten und letzten Schritt wird vom neuen Block die Hash-Referenz B2 erstellt. Sie ist erneut der kombinierte Hash-Wert aus Blockheader 2, Hash-Wurzel H34 und Hash-Referenz B1 auf dem Vorgängerblock. B2 stellt damit den neuen Kopf der aktualisierten Blockchain, bestehend aus vier Transaktionen, dar. Abbildung 12 zeigt den erreichten Zustand.

ABBILDUNG 13: VERÄNDERUNGEN IN BLÖCKEN FÜHREN ZU INKONSISTENTEN HASH-WERTEN.



Quelle: Eigene Darstellung

Abbildung 13 stellt dar, wie eine Veränderung an einer Transaktion (zum Beispiel, falls das Empfängerkonto oder die Menge des übertragenen Eigentums verändert wird) zu kaskadenartigen Fehlern führt. Durch das Ändern des Datensatzes H4 passt die Hash-Referenz H4 nicht mehr zu T4. Der Block ist damit ungültig, die Blockchain wurde korrumpiert und die Integrität ist nicht mehr gewährleistet. Sollte es dem Angreifer gelingen, auch die dazugehörige Hash-Referenz H4 passend zur modifizierten Transaktion T4 neu zu berechnen, wäre in der nächsten Stufe der Kaskade der Wurzel-Hash H34 ungültig, das heißt, der komplette Merkle Tree müsste neu berechnet werden. Dies führt dazu, dass auch der Hash-Wert B2 nicht mehr korrekt ist, somit müsste der komplette Block neu berechnet und der modifizierte Hash-Wert B2 an den Nachfolge-Block übergeben und auch dieser Block und alle in der Kette nachfolgenden Blöcke müssten neu berechnet werden. Im Folgenden wird gezeigt, dass solche Manipulationsversuche mit einem sehr hohen Preis verbunden sind, der aus wirtschaftlicher Perspektive (bewusst und konzeptbedingt) nicht rentabel ist.

↖ ERKENNEN VON MANIPULATIONEN

2.8 Kosten zur Aufrechterhaltung der Integrität

ZUSAMMENFASSUNG

» **Die Integrität der Blockchain als Datenspeicher ist durch mehrere Komponenten/Konzepte abgesichert. Das Verwenden einer veränderungssensitiven Datenstruktur ermöglicht das einfache und schnelle Erkennen selbst kleinster Änderungen. Mit der Konzeptionierung als „Nur-Lese-Speicher" beziehungsweise, wenn Editierungen notwendig sind, als „Nur-Anfüge-Speicher" sind ausschließlich Änderungen am Kopf der Kette erlaubt. Sehr rechenintensive und mit hohen Kosten verbundene Einfüge-Operationen machen Manipulationen unwirtschaftlich. Ein Wettrennen der Teilnehmer um das Finden eines gültigen Hashes zur Absicherung und zum Versiegeln eines neuen Blocks setzt die Teilnehmer einem Wettbewerb aus, dessen Schwierigkeit dynamisch an die Rechenleistung des Netzwerks angepasst wird.[10] Durch das Verteilen der Transaktionshistorie auf Tausende von Computern im Blockchain-Netzwerk (wir befinden uns hier in einem rein verteilten Peer-to-Peer-System) existieren simultan zahlreiche Kopien des verteilten Hauptbuches, die für eine erfolgreiche (aber nahezu unmögliche) Manipulation alle unbemerkt gefälscht/ersetzt werden müssten. Trotz der dezentralisierten Natur rein verteilter Blockchains sind theoretisch verborgene Zentralisierungen möglich.**

> „In jeden neuen Datensatz (‚block') wird eine kryptografische Prüfsumme (Hashwert) der bisherigen Kette (‚chain') von Datensätzen geschrieben, sodass eine Manipulation der Daten durch einzelne Teilnehmer im Prinzip unmöglich ist. Jeder neue Block wird durch ein dezentrales Konsensverfahren geschaffen und an die Blockchain angehängt, durch das die Reihenfolge der Datensätze in der Blockchain festgelegt wird." (VDI Technologiezentrum, 2018, S. 2)

In Abschnitt 2.4 wurde das in der (Bitcoin-)Blockchain verwendete kryptografische Hash-Puzzle vorgestellt. Abschnitt 2.7 beschreibt, wie neue Transaktionen am Kopf der Blockchain angehängt werden und wie Daten in der Blockchain veränderungssensitiv gespeichert werden. Wie die Aufrechterhaltung der Integrität und der nachhaltige Schutz der Transaktionsdatenhistorie auch gegenüber nicht vertrauenswürdigen und gegebenenfalls sogar unehrlichen Teilnehmern in einem Blockchain-Netzwerk gewährleistet werden kann, zeigt dieser Abschnitt.

Die Blockchain ist als rein verteiltes Peer-to-Peer-System angelegt, das heißt, es ist für jedermann offen und zugänglich. Da sich unehrliche und ehrliche Teilnehmer zunächst nicht unterscheiden lassen, wurde die Transaktionsdatenhistorie von Anfang an als unveränderlich ausgelegt und kann so als vertrauenswürdige Quelle zur Dokumentation und Nachverfolgung von Eigentumsangelegenheiten dienen. Unveränderlichkeit bedeutet aber auch, dass Daten rückwirkend nicht mehr verändert werden können, die Blockchain ist daher ein schreibgeschützter Nur-Lese-Speicher, vergleichbar mit fälschungssicheren Dokumenten wie Personalausweisen, Geldscheinen, Zeugnissen, Führerscheinen und anderen durch Behörden ausgestellte unveränderliche Dokumente. Der Blockchain-Experte Jimmy Song schreibt hierzu:

> „The main thing distinguishing a blockchain from a normal database is that there are specific rules about how to put data into the database. That is, it cannot conflict with some other data that's already in the database (consistent), it's append-only (immutable), and the data itself is locked to an owner (ownable), it's replicable and available. Finally, everyone agrees on what the state of the things in the database are (canonical) without a central party (decentralized)." (Song, 2018)

FÄLSCHUNGEN WERDEN UNWIRTSCHAFTLICH

Da neue Daten nur am Kopf der Blockchain angehängt werden und damit zumindest am aktuellen Block Einfüge-Operationen (und damit lokale Änderungen) möglich sind, besteht der Grundgedanke nun darin, Änderungen (also auch Einfüge-Operationen) so teuer (genauer: rechenintensiv) zu gestalten, dass Manipulationen und das Einschleusen gefälschter Transaktionsdaten in die Transaktionsdatenhistorie unwirtschaftlich sind. Im Optimalfall sollen die Kosten für Manipulationen um ein Vielfaches höher liegen als der erhoffte Gewinn durch den Betrugsversuch. Deutlicher formuliert lässt sich festhalten, dass die Blockchain nicht nur einen „Nur-Lese-Speicher", sondern gleichzeitig einen „Nur-Hinzufügen-Speicher" darstellt.

Abschnitt 2.7 hat schematisch gezeigt, wie neue Daten (gebündelt im Daten-Hash-Baum eines Blocks) an den Kopf der Blockchain angefügt werden. Der Vorgang zum Berechnen der Hash-Referenzen ist zunächst nicht rechenintensiv, da eine Eigenschaft von Hash-Funktionen genau die schnelle Berechenbarkeit ist. Abschnitt 2.3 hat dargestellt, wie diese Berechnung mithilfe eines Hash-Puzzles und einer definierten Nebenbedingung für den Blockheader („Schwierigkeitsgrad") künstlich verkompliziert werden kann. Abschnitt 2.6 führte die Datenstruktur der Blockchain und insbesondere den Aufbau des Headers ein, der (unter anderem) aus folgenden Komponenten besteht:

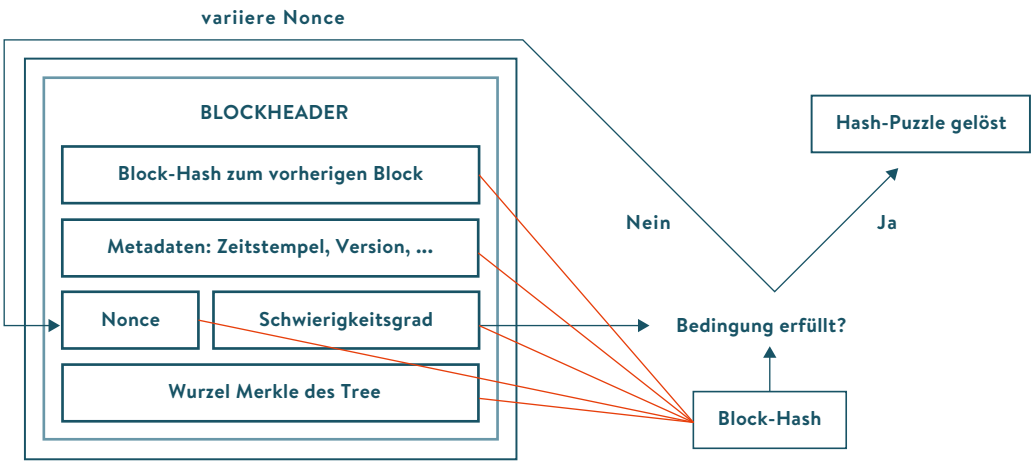
- Hash-Referenz auf den vorhergehenden Blockheader;
- Wurzel des Merkle Tree, in dem die (Transaktions-)Daten gespeichert sind;
- (verschiedene) Zeitstempel;
- Nonce-Feld;
- Schwierigkeitsgrad;

HASH-PUZZLE

Abbildung 14 zeigt, wie das Hash-Puzzle auf diesen Komponenten arbeitet. Aus den genannten Feldern wird ein kombinierter Hash-Wert berechnet. Dabei wird das Nonce-Feld so lange verändert, bis der gesamte Block-Hash der Bedingung des Schwierigkeitsgrades entspricht. Bemerkenswert ist zum einen, dass der Schwierigkeitsgrad Teil der Hash-Berechnung ist. Dies soll verhindern, dass bei einem Manipulationsversuch der Schwierigkeitsgrad künstlich herabgesetzt wird, um schneller an eine Lösung zu kommen. Zum anderen ist der Zeitstempel Teil des Hash-Puzzles, denn es soll im Block-Hash konserviert werden, dass der Zeitstempel des aktuell zu berechnenden Blocks nach dem Zeitstempel des Vorgängerblocks liegt (auch dies schützt vor Manipulationen).

ABBILDUNG 14: DIE VERSCHIEDENEN KOMPONENTEN DES HASH-PUZZLES

Ein Hash-Puzzle wird per Variationen im Nonce-Feld gelöst.



Quelle: Eigene Darstellung

Der Aufwand, der für das Finden eines gültigen Block-Hashes notwendig ist, ist abhängig vom Rechenaufwand, der für das Lösen des Hash-Puzzles betrieben werden muss. Zentrale Stellschraube hierfür ist der Schwierigkeitsgrad. In Abschnitt 2.4 wurde gezeigt, wie der Aufwand zum Finden einer validen Lösung quasi-exponentiell mit dem Erhöhen des Schwierigkeitsgrades steigt. Der Schwierigkeitsgrad wird dynamisch angepasst und hängt von der Rechenleistung ab, die zum jeweiligen Moment im Blockchain-Netzwerk zur Verfügung steht. Sind viele Peers als Teilnehmer im Netzwerk, wird der Schwierigkeitsgrad erhöht; stehen nur wenige Peers und damit wenig Rechenleistung zur Verfügung, so wird der Schwierigkeitsgrad gesenkt. Bei der Bitcoin-Blockchain ist die Vorgabe, dass rund alle zehn Minuten ein neuer Block erzeugt werden soll, und dementsprechend wird der Schwierigkeitsgrad zur Erfüllung der Block-Hash-Bedingung dynamisch für den nächsten Block geändert. So reagiert das System auf die zur Verfügung stehende Rechenleistung, indem es die Geschwindigkeit, mit der neue Blöcke entstehen, beobachtet und damit die Hash-Puzzles gelöst werden. Das Lösen dieser Hash-Puzzles wird Mining genannt (Genaueres hierzu im Abschnitt 2.9) und aufgrund der rechenintensiven Berechnung gültiger Hash-Werte werden gewaltige Mengen elektrischer Energie verbraucht. Je mehr Nonce-Werte durchprobiert werden, umso größer ist die Chance, einen passenden Block-Hash zu finden (vgl. Okupski, 2016). Wie das in der Realität aussieht, soll am Beispiel der Bitcoin-Blockchain gezeigt werden. Die Blockchain für die von Nakamoto entworfene Kryptowährung Bitcoin existiert seit Anfang 2009. Eine detaillierte Beschreibung dieser Kryptowährung würde den Rahmen der Arbeit überschreiten, aber einige Zahlen aus der Bitcoin-Blockchain helfen, die mittlerweile exorbitanten Dimensionen einzuschätzen. Seit 2009 ist diese Blockchain auf eine Größe von rund 221 Gigabyte angewachsen (vgl. Blockchain.com, 2019) und enthält rund 578.000 Blöcke (vgl. chaindex, 2019), in denen insgesamt über 140 Millionen Transaktionen verbrieft sind (vgl. Blockchain.com, 2019).

↖ SCHWIERIGKEITSGRAD

↖ DYNAMISCHES REAGIEREN AUF DIE AKTUELLE RECHENLEISTUNG DES NETZWERKES

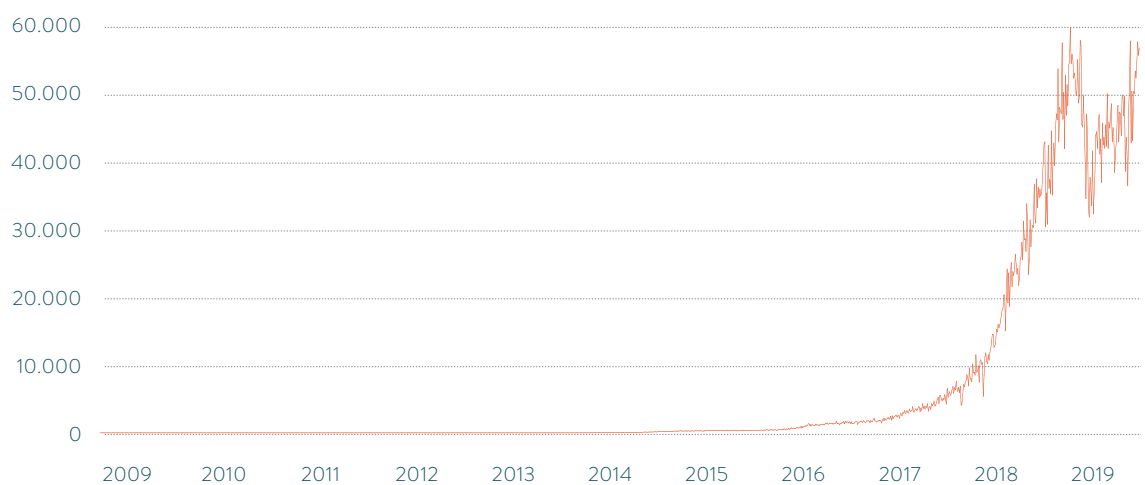
Noch bis vor wenigen Jahren konnten für die Berechnungen, um einen gültigen Hash-Wert für den aktuell anzuhängenden Block zu finden, gewöhnliche PCs eingesetzt werden – nach „ein paar Millionen“ Rechenoperationen war häufig der passende Hash-Wert gefunden. Aufgrund der mathematischen Eigenschaft bei der Ausführung von Hash-Funktionen entdeckten Teilnehmer, dass handelsübliche Computergrafikkarten wegen ihrer speziellen Hardware-Architektur diese Berechnung mehr als 100-mal so schnell ausführen konnten bei gleichzeitig verringertem Stromverbrauch (vgl. Fischer, 2017). Die Frage lautete nun nicht mehr, wie viele Rechenoperationen pro Sekunde, sondern wie viele Rechenoperationen pro Watt durchgeführt werden können. Mit dem explosionsartigen Anstieg der Rechenleistung passte sich auch die Schwierigkeit für das Hash-Puzzle an, sodass zunehmend sogenannte ASICs (application-specific integrated circuits) zum Einsatz kamen, die ausschließlich dafür entworfen und produziert worden sind, SHA256 zu berechnen (vgl. Tuwiner, 2017). Auch wenn die Rechenleistung des Bitcoin-Netzwerk in den letzten Monaten starken Schwankungen unterlag, liegt sie aktuell zwischen rund 42 und 59 Gigahertz pro Sekunde. Zum Vergleich: Bereits 2013 berichtete das englische Magazin Forbes: „Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!“ (vgl. Cohen, 2013). Und dementsprechend hoch war bereits 2013 der Stromverbrauch.

SPEZIAL-HARDWARE ZUR BERECHNUNG DER HASH-PUZZLES

ASICS SPEZIELL FÜR SHA256

ABBILDUNG 15: ENTWICKLUNG DER HASH-WERT-LEISTUNG DES BITCOIN-NETZWERKS

Die aktuelle Hash-Wert-Leistung des Bitcoin-Netzwerks knüpft an alten Bestmarken an.
Hash Rate, in TH/s, Januar 2009 bis Juni 2019



Quelle: Blockchain.info. Statistiken zur Bitcoin-Blockchain. Abgerufen am 06.06.2019 von https://blockchain.info/stats.

Die Internetseite Digiconomist führt den „Bitcoin Energy Consumption Index“ (vgl. Digiconomist, 2019) und schätzt, dass aktuell rund 190 Terrawattstunden (also Milliarden Kilowattstunden) pro Jahr auf die Berechnungen der Hashes und damit für die Absicherung der Integrität der Bitcoin-Blockchain aufgewendet werden.[11] Diese enormen Kosten entstehen nicht durch die Infrastruktur des Netzwerks selbst

190 TWH STROMVERBRAUCH PRO JAHR FÜR BITCOIN

(zum Beispiel durch Kosten für den Betrieb des dezentralen Netzwerks oder die Verwaltung des Hauptbuches), sondern aus dem kompetitiven Element und dem Anreizsystem, das Nakamoto für die Bitcoin-Blockchain gewählt hat. Wie dieses Incentivierungssystem funktioniert und warum die Teilnehmer an dieser Blockchain bereitwillig Stromkosten in Höhe von vielen Milliarden Euro aufbringen, wird Abschnitt 2.9 im Detail erläutern.

Zwei Besonderheiten bei der Aufrechterhaltung der Integrität sollen, wenngleich nur kurz, der Vollständigkeit halber erwähnt werden.

WIESO VERSCHWINDEN TRANSAKTIONEN AUS DER BLOCKCHAIN?

In verteilten Systemen sind die Daten auf den Nodes (Knoten) des Netzwerks nicht zu jeder Zeit synchron – beispielsweise aufgrund von Verzögerungen in der Kommunikation, gegebenenfalls auch Manipulationsversuchen oder durch das Einbringen ungültiger Transaktionen. Dennoch muss eine eindeutige und damit vertrauenswürdige Version der Blockchain existieren. Da zahlreiche Teilnehmer mit dem Finden und Abschließen gültiger Blöcke beschäftigt sind, kommt es gelegentlich vor, dass Lösungen simultan gefunden werden, das heißt, für kurze Zeit gibt es nicht nur eine Blockchain, sondern mehrere Versionen, die parallel weiterwachsen. Die Blockchain ähnelt zu diesem Zeitpunkt nicht mehr einer linearen Kette, sondern mehr einem Kaktus, an dessen Spitze verschiedene Verästelungen entstehen und die Kette im jeweiligen Ast parallel weiterwächst. Von „Zeit zu Zeit werden diese Äste bereinigt“[12] und es wird per Konsensentscheidung jener Ast für die Weiterführung der Transaktionsdatenhistorie ausgewählt, der maßgeblich zur Dokumentation von Transaktionen beiträgt, alle anderen Äste sowie die darin enthaltenen Transaktionen (Daten) werden verworfen, dem Netzwerk zur erneuten Prüfung (und gegebenenfalls Einfügen) zur Verfügung gestellt und die für diesen Pfad ausbezahlten Belohnungen zurückgefordert. Als Auswahlkriterium wird häufig das Maß der längsten Kette beschrieben, tatsächlich jedoch wird das Kriterium des höchsten Schwierigkeitsgrades angewendet. Die Information darüber, welche Schwierigkeit einem Block zugrunde gelegt wurde, ist im Header des jeweiligen Blocks beschrieben, die Schwierigkeit des Astes entspricht dann der Summe der kumulierten Schwierigkeiten der Blöcke dieses Pfades/Astes. Was wie ein Bug im Software-System oder wie „spukhaftes Verhalten“ erscheint, ist notwendiger Teil des Protokolls und zeigt, dass die Blockchain auch in diesem (konzeptionellen und technischen) Teil tatsächlich nicht unveränderlich ist.

51-PROZENT-ANGRIFF

Die zweite Besonderheit (die ebenfalls nur kurz angerissen werden kann) ist der Zustand der Eventual Consistency. Wächst einer dieser Äste schneller als die konkurrierenden Äste, so wächst auch die Wahrscheinlichkeit, dass dieser Ast als neuer Stamm fortgeführt und die anderen sich verzweigenden Äste verworfen werden. Hier setzt der sogenannte „51- Prozent-Angriff“ (vgl. Learn Cryptography, 2019) an. Dieser stellt den Versuch dar, gezielt manipulierte Transaktionen einzuschleusen und mit kumulierter Rechenleistung jenen Stamm dominant wachsen zu lassen, in dem diese gefälschten Daten eingebracht worden sind. Es wird also für eine kurze Zeit mit hohem Aufwand bewusst versucht, das dezentral angelegte System durch eine künstliche Zentralität zu beeinflussen. Das folgende Kapitel wird darstellen, dass – trotz der enormen Rechenleistung, die für einen solchen Angriff notwendig ist – unter bestimmten Voraussetzungen tatsächlich eine Konzentration und damit eine Zentralisierung von Mining-Leistungen beobachtet werden können (vgl. Kannenberg, 2014/2018).

ZENTRALISIERUNG VON MINING-LEISTUNGEN

2.9 Spieltheorie und Incentivierung

ZUSAMMENFASSUNG

» **Als letzter Baustein der Betrachtung der technischen und konzeptionellen Grundlagen der Blockchain wird die Incentivierung der Teilnehmer beschrieben, die notwendiges Element zur Aufrechterhaltung der Integrität der Blockchain ist. Eine regelbasierte Kombination aus Belohnung, Bestrafung und Wettbewerb macht die Teilnehmer eines dezentralen Systems gleichzeitig zu Kontrolleuren, die für ihre Überprüfungstätigkeit entlohnt werden.**

> „Jeder neue Block wird durch ein dezentrales Konsensverfahren geschaffen und an die Blockchain angehängt […]." (VDI Technologiezentrum, 2018)

↖ **PROOF OF WORK**

In Abschnitt 2.8 wurde gezeigt, wie mithilfe einer enormen Rechenleistung Hash-Werte im Bitcoin-Netzwerk zur „Versiegelung" neuer Blöcke von Transaktionen berechnet werden. Das in dieser Blockchain verwendete Konsensverfahren ist als Proof of Work ausgelegt und konzeptbedingt dient die geleistete Arbeit an einer Lösung (Hash-Wert-Berechnung) als Nachweis. Wie die Teilnehmer motiviert werden, diese Arbeit zu leisten und ihre Hardware und Stromkosten zur Verfügung zu stellen, wird im Folgenden dargestellt.

↖ **TEILNEHMER ALS KONTROLLEURE**

Die (Bitcoin-)Blockchain ist als offenes System ausgelegt, mit dem sich auch der unehrlichste Teilnehmer verbinden und Transaktionen erstellen kann. Die Aufgabe besteht also darin, das System offen für alle zu halten, aber gleichzeitig dafür Sorge zu tragen, dass nur gültige Transaktionen angehängt werden können. Die von Nakamoto beschriebene und in der Blockchain umgesetzte Lösung besteht darin, dass sämtliche Teilnehmer im System als Kontrolleure arbeiten und die Gültigkeit dieser Transaktionen prüfen und autorisieren. Fehlerhafte Transaktionen werden bestraft und die Bestätigung gültiger Transaktionen wird belohnt. Dabei werden Elemente der Spieltheorie eingesetzt, indem die Teilnehmer einem gegenseitigen Wettbewerb ausgesetzt werden. Wer über die vollständig und lückenlos dokumentierte Transaktionshistorie die Gültigkeit einer aktuell eingetragenen Transaktion nachweisen kann, wird mit Bitcoins belohnt. Jede Bitcoin-Transaktion kann mit einer Transaktionsgebühr versehen werden, über deren Höhe die Priorität bei der Abarbeitung durch die Teilnehmer gesteuert werden kann.[13] Mehrere Tausend Transaktionen werden dann durch die Teilnehmer auf Gültigkeit geprüft, zu einem Block zusammengesetzt und per Hash-Puzzle als versiegelter Block an den Kopf der Blockchain angehängt. Die Belohnung besteht aus der Summe der Transaktionsgebühren in diesem Block und der Belohnung für das Finden eines gültigen Block-Hashes. Wie hoch die Belohnung für den Block-Hash ist, wurde ebenfalls von Nakamoto festgelegt. So wurden zu Beginn der (Bitcoin-)Blockchain 50 Bitcoins für das Abschließen eines Blocks an den Teilnehmer, der den Hash findet, ausgeschüttet. Im Bitcoin-Protokoll ist jedoch festgelegt, dass diese Belohnung alle 210.000 Blöcke halbiert wird. Nach heutigem Stand befinden sich in dieser Blockchain 578.000 Blöcke und die Block-Reward beträgt aktuell 12,50 Bitcoins. Diese Belohnung ist eine weitere Funktion des Minings und dient der Erzeugung von neuen Geldeinheiten im Bitcoin-System, vergleichbar mit der Funktion einer Zentralbank. Im Unterschied zur Zentralbank ist im Protokoll der Blockchain (der Kryptowährung) ein festes Erzeugungsschema hinterlegt, um einer möglichen Inflation entgegenzuwirken, sodass Einheiten nicht willkürlich generiert werden können. Diese neu erzeugten

Geldeinheiten werden demjenigen, der das Block-Puzzle erfolgreich löst, gutgeschrieben. Um mit der detaillierten Ausführung dieses Vorgangs den Rahmen der Arbeit auch an dieser Stelle nicht zu überschreiten, kann erwähnt werden, dass bei einem derzeitigen Bitcoin-Kurs von rund 6.500 Euro pro Bitcoin die Belohnung als Summe von Transaktionsgebühren und Lösen des Hash-Puzzles bei rund 80.000 Euro pro Block liegt (vgl. BitInfoCharts, 2019).
Die spieltheoretischen Elemente bei diesem Prozess bestehen aus einer Kombination von Belohnen, Bestrafen, Kontrollieren und dem Wettbewerb sowie den entsprechenden Regeln, auf denen diese Elemente basieren. So wird in einem System, in dem per se Misstrauen und Vertrauen miteinander konkurrieren, Missbrauch geahndet und Ehrlichkeit belohnt.

Das Element der Belohnung besteht also in der Bezahlung der Teilnehmer für die übernommene Arbeit und dem Bereitstellen von Energie, (Rechen-)Zeit und Investition zur Absicherung der Integrität der Blockchain. Das zweite Element, die Bestrafung, ist ein Mittel, das Verhalten (unehrlicher) Teilnehmer zu ahnden, die die Integrität der Blockchain durch Manipulation, das Melden falscher Hash-Werte oder das Einschleusen falscher Transaktionen gefährden. Werden solche Vorgänge vom Netzwerk erkannt, wird die Belohnung wieder zurückgefordert und die investierten Kosten waren umsonst. Damit besteht die Bestrafung darin, trotz hoher Investitionen keine Belohnung zu erhalten. Da die Blockchain dezentral als rein verteiltes Peer-to-Peer-System ausgelegt ist, gibt es keine zentrale Instanz, die eine Kontrollfunktion übernimmt und richtige (ehrliche) von falschen (unehrlichen) Lösungen unterscheidet. Diese Funktion übernehmen die Teilnehmer selbst, indem sie Lösende und Kontrollierende gleichzeitig sind. Wird eine (erste) Lösung eingereicht, so wird die Rolle der Teilnehmer vertauscht, sie kontrollieren nun die gefundene Lösung. Die Belohnung besteht ab jetzt darin, Fehler der anderen Teilnehmer aufzudecken. Ist die Lösung fehlerhaft, bekommen die Kontrolleure die Belohnung und die Einreichenden werden bestraft. Die Teilnehmer befinden sich in einem permanenten Wettlauf, Transaktionen auf Gültigkeit zu prüfen, einen gültigen Block-Hash zu berechnen und diese Lösung als Erster einzureichen, die dann wiederum in einem gleichen Wettbewerb auf Korrektheit geprüft wird. Der spieltheoretische Ansatz basiert auf einem Geschwindigkeits- sowie Qualitätswettbewerb und der Annahme, dass die ehrlichen Benutzer überwiegen und darauf aus sind, die (hohe) Belohnung zu erhalten.

↖ KOSTEN ZUR ABSICHERUNG DER INTEGRITÄT DER BLOCKCHAIN

↖ EHRLICHE UND UNEHRLICHE TEILNEHMER IM WETTBEWERB

↖ GESCHWINDIGKEITS- UND QUALITÄTS-WETTBEWERB

Kapitelendnoten

1 Der Begriff der Disintermediation beschreibt einen Bedeutungsverlust von Vermittlern zwischen verschiedenen Akteuren in einem Wirtschaftssystem.

2 Nakamoto verwendete den Begriff Blockchain selbst nicht in seinem Artikel. Der Begriff leitet sich aus der Art und Weise ab, wie Datensätze linear verkettet werden.

3 Kryptografische Hash-Funktionen werden oft auch als kryptologische Hash-Funktionen bezeichnet.

4 MIT Laboratory for Computer Science and RSA Data Security, Rivest, R. (1992). The MD5 Message-Digest Algorithm. Abgerufen am 29.05.2019 von https://tools.ietf.org/html/rfc1321.

5 In der Kryptografie wird der Begriff Nonce (Abkürzung für „used only once") häufig benutzt, um Zahlen- oder Buchstabenkombinationen zu beschreiben, die nur ein einziges Mal im lokalen Kontext verwendet werden sollen. Siehe auch: Needham, R. M. und Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. Palo Alto: Xerox Palo Alto Research Center.

6 Auf der Internetseite https://www.md5-generator.de kann der Leser selbst versuchen, ein solches Hash-Puzzle zu lösen. Aufgabe: Finden Sie einen beliebigen Text, der einen Hash-Wert (MD5-Zeichenkette) mit einer, zwei oder sogar drei führenden Nullen erzeugt.

7 In der Informationstechnik wird der Teil der Daten, der Zusatzinformationen bzw. Nutzinformationen enthält, oft an den Anfang eines Datenblocks gesetzt und damit als „Header" bezeichnet.

8 Der so erzeugte Block-Hash muss die Bedingung des Schwierigkeitsgrades erfüllen.

9 Unter diesem Link kann z. B. der Block Nr. 523999 aus der Bitcoin-Blockchain eingesehen werden: https://blockchain.info/de/block/000000000000000003f9b5d372cce4b117bb7a8e24a9f094d8a395276fc59ef

10 Diese Anpassung erfolgt im Bitcoin-Netzwerk automatisch alle zwei Wochen.

11 Der IT-Sicherheitsexperte Marc Bevand hat zur Bestimmung der Profitabilität von Mining neben den Stromkosten auch die Kosten für Spezialhardware (ASICs) mit einberechnet und kommt zu dem Schluss: „When considering the big picture I believe Bitcoin mining is not wasteful due to the various benefits." Siehe: Bevand, M. (2016). Bitcoin Mining is Not Wasteful. Abgerufen am 29.05.2019 von http://blog.zorinaq.com/bitcoin-mining-is-not-wasteful/.

12 Dies stellt eine grobe Vereinfachung des Vorgangs dar, ist aber für das Verständnis an dieser Stelle ausreichend.

13 Die aktuell üblichen Transaktionsgebühren können auf der Seite https://live.blockcypher.com/btc/ eingesehen werden.

03

DER SOZIOTECHNISCHE CHARAKTER DER BLOCKCHAIN

Dieses Kapitel erörtert Merkmale, Eigenschaften, Errungenschaften, aber auch Nachteile der Blockchain. Ebenfalls werden typische Blockchain-Anwendungen, Anwendungsfelder und beispielhaft konkrete kommerzielle Beispiele erläutert. Das Kapitel schließt mit aktuellen Weiterentwicklungen, Modifikationen und Alternativen zur Blockchain und greift Fragen zur Anforderungsgestaltung auf.

Abschnitt 3.1 entwickelt zunächst die technischen Eigenschaften und charakteristischen Vorzüge von Blockchain-Anwendungen. Abschnitt 3.2 diskutiert die Beschränkungen der Blockchain, die teilweise bereits in der Technologie selbst angelegt sind oder die aus einem bisher fehlenden passenden gesellschaftlichen (Rechts-)Rahmen oder aus sozioökonomischen Dynamiken resultieren. Abschnitt 3.3 arbeitet zentrale Prinzipien und Nutzenversprechen heraus, die aus gesellschaftlicher Perspektive leitend sein können, diesen Beschränkungen zu begegnen und die technischen wie gesellschaftlichen Potenziale der Blockchain zum allgemeinen Nutzen zur Geltung zu bringen. Abschnitt 3.4 führt eine kritische Diskussion dieser Prinzipien und ihrer Realisierbarkeit. Abschnitt 3.5 führt ein in die elementaren Anwendungen, die eine wesentliche Grundlage der in Abschnitt 3.6 vorgestellten prominenten Blockchain-Projekte und Architekturen bilden. Diese informieren und motivieren zugleich, die in den ersten Abschnitten entwickelten Spannungsfelder in Abschnitt 3.7 anhand soziotechnischer Typen von Blockchains zu manifestieren. Wie einzelne Blockchains oder die Technologie im Ganzen sich in diesen Spannungsfeldern weiterentwickeln beziehungsweise weiterentwickeln werden können, ist Gegenstand des Abschnitts 3.8. Schließlich stellt Abschnitt 3.9 zusammenfassend die auch in diesem Bericht adressierten offenen Forschungsfragen dar.

3.1 Technische Eigenschaften von Blockchain-Anwendungen

Zu den technischen Eigenschaften von Blockchain-Anwendungen zählen:

» Sicherheit und Integritätserhaltung

INTEGRITÄTSERHALTUNG UND SCHUTZ VOR MANIPULATIONEN

Die Sicherheit der Blockchain basiert auf zwei Betrachtungsperspektiven: Zum einen kann die Sicherheit auf Ebene der Transaktionen gewährleistet werden, da das Eigentum nur vom rechtmäßigen Eigentümer verwaltet und gegebenenfalls übertragen werden kann. Der Nachweis wird unter anderem über die prüfbare Transaktionshistorie und die Tatsache, dass nur der Eigentümer den privaten Schlüssel besitzt, erbracht. Zudem wird das Gesamtsystem über eine veränderungssensitive Datenstruktur vor Manipulationen oder Veränderungen der Transaktionshistorie, des zentralen Hauptbuches geschützt und so die Datenintegrität aufrechterhalten.

» Zuverlässigkeit und Belastbarkeit

Die Blockchain ist für die Prüfung und Übertragung von Eigentum eine zuverlässige und belastbare Quelle. Sie ist fälschungssicher beziehungsweise gegen Angriffe unterschiedlichster Art resistent und damit vertrauenswürdig (zumindest solange der Großteil der Teilnehmer ehrlich ist, siehe hierzu Abschnitt 2.8 zum 51-Prozent-Angriff).

» Offenheit und Transparenz

Die Blockchain (in der Form, wie sie hier vorgestellt worden ist) ist ein offenes System, das jeder einsehen und an dem jeder partizipieren kann, sowohl als Eigentümer, Verwalter, Miner oder Kontrolleur. Transaktionen sind ebenso wie der aktuelle Status der Blockchain selbst offen einsehbar.[14]

» Pseudonymität

Die Operationen auf der Blockchain sind zwar öffentlich einsehbar, doch die Sender- und Empfängeradressen sind über Hash-Werte kodiert (siehe Abschnitte 3.4 und 3.5). So lassen sich Transaktionen nachverfolgen (zur Abklärung des Eigentums eine zwingende Notwendigkeit) und zum Beispiel das Problem des „Double-Spendings“ (Chohan, 2017) vermeiden. Welche realen Personen sich jedoch hinter den kodierten Adressen befinden, kann nur mit Mitteln außerhalb der Blockchain herausgefunden werden beziehungsweise wenn die Kryptowährungen über ein reales Konto in FIAT-Währung umgetauscht wird oder wenn Personen öffentlich ihre Einzahlungsadresse bekanntgeben.[15] Die (Bitcoin-)Blockchain ist also nicht anonym, sondern pseudonym.[16]

» Unveränderlichkeit, Zensur und Regulierung

Als rein verteiltes Peer-to-Peer-System unterliegt die Blockchain keiner zentral verwaltenden Instanz. Transaktionen können auch durch regulierende Entitäten nicht verändert oder gegebenenfalls zensiert werden. Wissenschaftler der Universitäten in Aachen und Frankfurt am Main haben den Inhalt der Bitcoin-Blockchain untersucht und dabei versteckten illegalen Content entdeckt:

> „Bitcoin’s blockchain contains at least eight files with sexual content. While five files only show, describe, or link to mildly pornographic content, we consider the remaining three instances objectionable for almost all jurisdictions: Two of them are backups of link lists to child pornography, containing 274 links to websites, 142 of which refer to Tor hidden services.“ (Matzutt et al., 2018)

Die Eigenschaft der Unveränderlichkeit der Blockchain scheint in solchen Fällen zu einem Problem zu werden (vgl. Dölle, 2018).

» Hochverfügbarkeit

Im Gegensatz zu zentralisierten Systemen, bei denen gegebenenfalls Wartungspausen im System eingelegt werden, Systemupdates oder erwünschte Unterbrechungen im Betriebsablauf stattfinden können, läuft die Blockchain ununterbrochen. Zahlreiche Kopien und Instanzen werden sekündlich erweitert, geprüft, verworfen und (irgendwann) konsistent und unveränderlich angefügt. Fallen einzelne Knoten aus, übernehmen andere Knoten ihre Funktion. Das Netzwerk verändert sich permanent, indem neue Teilnehmer hinzukommen oder andere Teilnehmer aus dem Netzwerk austreten. Diese Hochverfügbarkeit schützt vor Datenverlust, verhindert aber auch das (ungewollte oder gewollte) Abschalten des Gesamtsystems und entzieht sich somit regulierenden Eingriffen.

3.2 Soziotechnische Beschränkungen der Blockchain

Die Blockchain ist über die raffinierte Verknüpfung bekannter und bewährter Basistechnologien in Kombination mit spieltheoretischen Elementen eine äußerste robuste Technologie, doch sie ist nicht frei von Beschränkungen. Diese Beschränkungen führen auch dazu, dass der Einsatz einer Blockchain vertieft abgewogen werden muss. Ebenso können die zunächst positiven Eigenschaften nachhaltige Hürden darstellen, die sie für bestimmte Anwendungszwecke ungeeignet machen.

3.2.1 TECHNISCHE BESCHRÄNKUNGEN

Sicherheit

Antagonistisch zum eben beschriebenen Sicherheitsvorteil unterliegt die Blockchain hier auch einer Beschränkung. Zum einen ist der Eigentümer alleiniger Verwalter seiner Daten. Durch das Wegfallen einer zentralen verwaltenden Instanz (wie beispielsweise einer Bank) obliegt dem Benutzer mit dem Schutz seines privaten Schlüssels (siehe Abschnitt 2.4) die exklusive Verantwortung. Wird der Schlüssel gestohlen oder kommt er abhanden, so hat der Benutzer keinen Zugriff mehr auf seine Daten, da er sich mit dem privaten Schlüssel als Eigentümer autorisiert. Ein Neuausstellen des (gleichen) Schlüssels, vergleichbar mit dem Zurücksetzen eines Passwortes bei einem Dienstleister, ist nicht mehr möglich (vgl. Gruenderszene.de, 2018).

Zudem basiert das gesamte Sicherheitsmodell auf der Annahme, dass die verwendeten kryptografischen Hash-Funktionen sicher, also zum Beispiel robust gegenüber Kollisionen sind. In der Vergangenheit mussten kryptografische Hash-Funktionen wie beispielsweise MD5 oder SHA1 durch die Entwicklung neuer Angriffsvektoren als unsicher eingestuft werden. Mit der Entwicklung von Quantencomputern steigt auch das Sicherheitsrisiko für Blockchains. Forscher warnen vor den Gefahren, zeigen aber auch gleichzeitig Möglichkeiten auf, wie Blockchains künftig quantensicher gestaltet werden können (vgl. Aggarwal et al., 2017).

↖ QUANTENSICHERE BLOCKCHAINS

Eingeschränkte Skalierbarkeit

Die Blockchain passt die Schwierigkeit für die Lösung der Hash-Puzzles dynamisch an die Rechenleistung des Netzwerks an. Eine der Vorgaben im Bitcoin-Protokoll lautet unter anderem, dass rund alle zehn Minuten ein neuer Block entstehen soll. Da die Blockgröße auf 1 Megabyte und damit die Anzahl der Transaktionen auf wenige Tausend Transaktionen pro Block begrenzt ist, resultiert daraus eine Obergrenze von rund sieben Transaktionen pro Sekunde (vgl. Swan, M., 2015). Die Blockchain skaliert

zwar mit der Anzahl der Nutzer, aber nicht bei der Transaktionsgeschwindigkeit, denn die Absicherung der Blockchain durch einen Proof-of-Work-Konsensalgorithmus in Verbindung mit der gewählten Blockgröße reduziert (konzeptbedingt) die Verarbeitungsgeschwindigkeit der Transaktionen. Diese reduzierte Verarbeitungsgeschwindigkeit führte Ende 2017, in der jüngsten Spekulationshochphase der Kryptowährung Bitcoin, zu sehr hohen Gebühren, die zeitweise über 50 US-Dollar pro Transaktion betrugen, denn um die Verarbeitung von Transaktionen zu beschleunigen, wurden hohe Transaktionsgebühren von den Teilnehmern geboten, um den jeweiligen Transfer für die Miner attraktiv zu machen und die Abwicklung der eigenen Transaktionen auf diese Weise zu beschleunigen.

3.2.2 BESCHRÄNKUNGEN DER BLOCKCHAIN IM KONTEXT DER DSGVO

Mit der am 25. Mai 2018 in Kraft getretenen Datenschutzgrundverordnung (DSGVO) der Europäischen Union wurden zahlreiche neue Rechte und Pflichten für Daten erfassende und verarbeitende Organisationen eingeführt. Prinzipiell kann die DSGVO als Stärkung der Position der Blockchain-Technologie aufgefasst werden, da Konzepte wie Selbstbestimmung und Datenminimierung leitgebend für die Verordnung sind. Allerdings wurde die Blockchain-Technologie selbst bei der Genese der DSGVO nicht berücksichtigt. Die in der DSGVO verankerten Rechte werden ausschließlich natürlichen Personen gewährt. Folglich sind momentan nur Anwendungen von Blockchain betroffen, bei denen die Daten natürlicher Personen gespeichert werden.

Zunächst sind die offene Architektur und der transparente (Lese-)Zugriff auf Daten eine notwendige Voraussetzung für die korrekte Funktionsweise der Blockchain. Doch die Offenheit der Daten kann – vor allem für EU-Bürger – aus datenschutzrechtlicher Sicht ein Bedrohungspotenzial für das Recht auf Schutz von Privatsphäre und personenbezogenen Daten darstellen (vgl. Deloitte, 2019). Der Blockchain Bundesverband hat in einem am 25. Mai 2018 veröffentlichten Positionspapier (vgl. Blockchain Bundesverband, 2018) verschiedene Konflikte zwischen der 2016 beschlossenen DSGVO und der Blockchain herausgearbeitet und bemerkt in diesem Papier:

> „It is important to note that pseudonymized data are personal data: […] Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. […] Conclusion: It is clear that any data that is stored on a blockchain can constitute personal data. To minimize overlap and potential conflict with the GDPR, developers must limit the amount of personal data stored on blockchain, find new ways to anonymize data, and seek out GDPR-compliant off-chain data storage options.“[17] (Blockchain Bundesverband, 2018)

Ferner konstatiert das Papier: „Blockchains and other decentralized technologies do not fit cleanly in this model (The GDPR data protection model).“[18] (Blockchain Bundesverband, 2018).

Dies kann zusammengenommen insbesondere bei folgenden Aspekten zu einer erheblichen Rechtsunsicherheit führen:

- die Bestimmung der „Verantwortlichen“ (controller) von Blockchains im Sinne des Artikel 4 Nummer 7 DSGVO;[19]
- die Frage, welche Daten im Kontext einer Blockchain als pseudonymisiert gelten;
- die Frage, was als DSGVO-konforme Umsetzung des Rechts auf Löschung („Recht auf Vergessenwerden“) für eine Blockchain gilt.

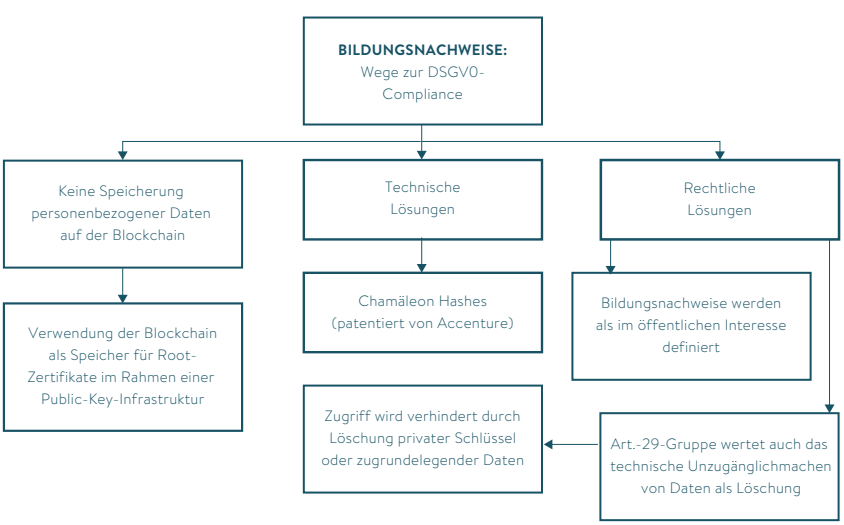
Vorausgesetzt, dass die EU keine gesonderte Blockchain-Richtlinie in die bestehende DSGVO integriert, ist zunächst davon auszugehen, dass diese Fragen durch Leitlinien und Empfehlungen des Europäischen Datenschutzausschusses sowie die Rechtsprechung in den EU-Mitgliedstaaten geklärt werden. Nach Ansicht der Autoren wird die Stoßrichtung solcher Auslegungen stark davon abhängen, ob die jeweiligen Akteure Anreize für den Einsatz der Blockchain-Technologie schaffen möchten oder nicht. Die Frage, ob die Blockchain-Technologie die Bestimmungen der DSGVO erfüllt, ist somit zur Zeit nicht nur rein rechtlicher Natur und sie muss momentan vor allem auch politisch beantwortet werden.

↖ **DSGVO-KOMPATIBILITÄT**

Obwohl wir in diesem Abschnitt auf mögliche Auswirkungen der DSGVO auf die Blockchain-Technologie verweisen, übersteigt eine detaillierte Analyse der rechtlichen Situation oder gar eine Rechtsberatung den Rahmen der vorliegenden Studie. Nichtsdestoweniger legen erste Analysen des rechtlichen, politischen und technologischen Umfelds nahe, dass es mehrere mögliche Wege gibt, Blockchain mit der DSGVO zu vereinbaren (siehe Abbildung 16). So wird beispielsweise das Recht auf Löschung allgemein als große Herausforderung im Kontext der DSGVO angesehen, da Blockchains per Definition unveränderlich sind. Dies könnte adressiert werden,

- indem in Blockchains nur Daten über juristische und nicht über natürliche Personen gespeichert werden,
- indem neue Arten von Blockchains entwickelt werden, die die Löschung unter bestimmten Umständen erlauben – beispielsweise mittels sogenannter „Chamäleon-Hash-Funktionen“ (vgl. Krawczyk/Rabin, 2000), die unter bestimmten (engen) Bedingungen die Veränderung von Blockchain-Einträgen ermöglichen (vgl. Erbguth, 2018),
- indem festgelegt wird, dass die Speicherung bestimmter Daten zum Beispiel im Hochschulbildungssystem mittels Blockchain im öffentlichen Interesse liegt,
- indem festgelegt wird, ob die dauerhafte Unzugänglichmachung von Daten rechtlich bereits als Löschung angesehen werden kann.

ABBILDUNG 16: ANSÄTZE ZUR DSGVO-COMPLIANCE



Quelle: eigene Darstellung

3.2.3 SOZIOÖKONOMISCHE BESCHRÄNKUNGEN DER BLOCKCHAIN

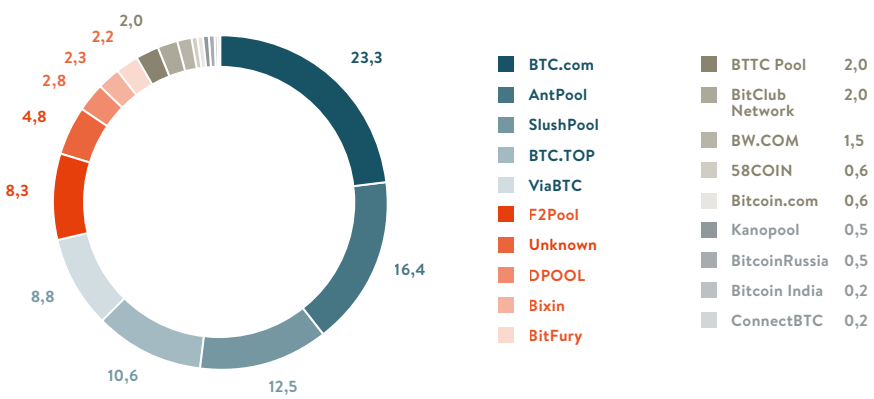
Versteckte Zentralität

Aufgrund der enormen Rechenleistung, die mittlerweile für das Lösen des Hash-Puzzles benötigt wird, schalten sich Teilnehmer zu sogenannten Mining-Pools zusammen, um mit gebündelter Leistung die Wahrscheinlichkeit zu vergrößern, den Wettbewerb (wie in Abschnitt 2.9 beschrieben) für sich zu entscheiden und den Gewinn unter sich aufzuteilen. Aufgrund der zunehmenden Notwendigkeit, sehr teure Spezial-Hardware (ASICs) einsetzen zu müssen, entstehen Gruppen, die sich zu Oligopolen zusammenschließen. Abbildung 17 zeigt die Verteilung von Mining-Pools und wie die größten drei Pools mehr als 50 Prozent der Rechenleistung im Bitcoin-Netzwerk stellen. Obwohl das Netzwerk als rein verteiltes Peer-to-Peer-System (vgl. Abschnitt 2.2, ein Netzwerk „Gleicher unter Gleichen“) auf Heterogenität der Teilnehmer ausgelegt ist, führen diese Strukturen zu einer unerwünschten Quasi-Zentralisierung durch einzelne Gruppen (vgl. Giese, 2018).

Dabei sind mehr als 70 Prozent der Mining-Pools und damit der Rechenleistung des Bitcoin-Blockchain-Netzwerks in China ansässig (vgl. Tuwiner, 2018). Einer der Gründe hierfür sind zum Beispiel die sehr niedrigen Energiepreise aus fossilen Quellen (vgl. Peck, 2017).

ABBILDUNG 17: MARKTANTEIL DER GRÖSSTEN BITCOIN MINING POOLS

in Prozent



Quelle: Tuwiner, J. (2018). Bitcoin Mining in China. Abgerufen am 29.05.2019 von https://www.buybitcoinworldwide.com/mining/china/.

Kosten und Größe

Die Kosten für den Betrieb der Bitcoin-Blockchain entstehen nicht durch die Infrastruktur des Netzwerks selbst (zum Beispiel Kosten für den Betrieb des dezentralen Netzwerks oder die Verwaltung des Hauptbuches), sondern sind durch das kompetitive Element des Lösens der Hash-Puzzles sowie die begrenzte Skalierbarkeit bedingt. Die Internetseite Digiconomist schätzt die jährlichen Kosten für das Mining auf rund 3,5 Milliarden US-Dollar (vgl. Digiconomist, 2019). Abschnitt 2.8 hat

dargestellt, dass diese Kosten bewusst hoch gehalten werden und ein Teil der Sicherstellung der Integrität sind. Die Größe der gesamten Blockchain, bestehend aus aktuell mehr als 578.000 Blöcken, beträgt derzeit fast 221 Gigabyte. Diese Daten werden im Peer-to-Peer-System auf unzähligen Computern verwaltet, denn jeder Teilnehmer ist in der Lage, eine vollständige Kopie vorzuhalten und bei Bedarf einen sogenannten „Full Node" zu betreiben (vgl. Bitcoin Wiki, 2019). Die hohe Redundanz hat somit auch hinsichtlich der Größe des „Distributed Ledger" einen Preis, den es mit Speicher- und Transfervolumen zu bezahlen gilt.

Flexibilität

Die in Kapitel 2 dargestellten Basistechnologien sind in der Blockchain auf eine bewusste Art und Weise zu einem komplexen System zusammengefügt. Das Gesamtsystem stellt ein ausgeglichenes digitales Ökosystem dar, das in dieser Form schon seit fast zehn Jahren weitestgehend unverändert sowie autonom und unreguliert funktioniert. Die Regeln sind im Quellcode beziehungsweise im Protokoll festgelegt und in der Blockchain unveränderlich verankert. Tiefgreifende Veränderungen würden die Blockchain ungültig machen und eine Neuberechnung der kompletten Transaktionsdatenhistorie nach sich ziehen. Abschnitt 3.8 wird zeigen, dass Veränderungen zwar möglich sind, aber hierfür ein hoher Preis gezahlt werden muss, denn auch Veränderungen unterliegen dem Konsens der gesamten Teilnehmer, sodass Änderungen der Zustimmung durch mehr als die Hälfte der Teilnehmer bedürfen. Im Vergleich zu Datenbanken und anderen zentral angelegten Strukturen ist die Blockchain deutlich weniger flexibel.

Juristische Anerkennung und Einordnung

Die Blockchain ermöglicht es Anwendern, dezentral und frei von Regulierungsinstanzen unter anderem Eigentum zu verwalten. Je nach Einsatzgebiet sind dabei zahlreiche juristische Fragen offen, denn durch die vielfältigen Einsatzmöglichkeiten der Blockchain können die unterschiedlichsten Rechtsbereiche betroffen sein. Von zivil- und datenschutzrechtlichen bis hin zu regulierungsrechtlichen Fragen berührt diese Technologie an verschiedenen Stellen Grundlagen unseres Rechts. Eine nähere Betrachtung würde den Rahmen dieser Arbeit überschreiten.

Nutzerakzeptanz

Die in der Blockchain verwendeten Technologien und Konzepte sind komplex. Ein Großteil der Menschen (und auch der Benutzer) versteht nicht, wie die Blockchain technisch funktioniert. Da Intermediäre fehlen und somit keine Dienstleister bei der Verwaltung des Eigentums helfend zur Verfügung stehen (zum Beispiel der Bankangestellte am Schalter, zu dem ein Kunde im Zweifel gehen kann, oder eine Hotline bei der Verwaltung des Handy-Vertrages), verursacht dies eine große Unsicherheit bei den Benutzern. Auch rechtliche Unsicherheiten und der Umgang von Behörden mit der neuen Technologie (Beispiel: Versteuerung von Gewinnen aus dem Handel mit Kryptowährungen oder wie gehen Behörden mit digitalen Währungen um, die keinen realen Gegenwert haben?) spielen eine Rolle bei der mangelnden Nutzerakzeptanz.

Zwar lassen sich einige Beschränkungen der Blockchain durch konzeptionelle Änderungen überwinden, doch müssen hierzu Konflikte mit grundlegenden Paradigmen gelöst werden (beispielsweise der Unveränderlichkeit). So soll beispielsweise ein bevorstehendes Software-Update des Bitcoin-Netzwerks das System massentauglich machen und wesentlich mehr Transaktionen bei geringeren Gebühren ermöglichen (vgl. Kilic, 2018; Poon/Dryja, 2016).

3.3 Soziotechnische Mehrwerte der Blockchain

3.3.1 GESELLSCHAFTLICHE WERTE UND ALLGEMEINNUTZEN

Dezentralisierung

Dezentralisierung im Rahmen der Blockchain-Governance bedeutet die Verlagerung der Kontrolle von Ledgern (Hauptbüchern) von zentralen Akteuren (Intermediären) auf ein dezentrales Netzwerk von Stakeholdern als „Gleiche unter Gleichen". Eine solche Dezentralisierung bedeutet, dass zentrale Parteien die Möglichkeit verlieren, diese Daten direkt zu ändern, den Zugriff darauf einzuschränken oder zu nutzen. Dies gilt auch für Behörden, die als zentrale Datenverarbeiter fungieren. Mithin wird dabei die Rolle des Intermediärs nicht aufgelöst, sondern in ein digitales, regelbasiertes System überführt, in dem Korrektheit und Vertrauen über die Teilnehmer erzeugt werden unter der Annahme, dass die meisten Teilnehmer eines solchen Netzwerks ehrlich sind. Diese Verlagerung weg von dedizierten Vermittlungsinstanzen (Banken, Notare, gegebenenfalls auch Behörden) hinein in die Blockchain schafft ein neuartiges Vertrauen in Technik, Protokolle und rechnergestützte Konsensentscheidungen (vgl. The Economist, 2015) und führt aus sozialwissenschaftlicher Perspektive möglicherweise zu einem gesellschaftlichen und technischen Paradigmenwechsel im Umgang mit Eigentum und Organisationen.

Informationelle Selbstbestimmung

Volle informationelle Selbstbestimmung (self-sovereignty) bedeutet, dem Benutzer die volle und direkte Kontrolle über seine Daten zu geben und ihm die Entscheidung zu überlassen, wie und wo diese Daten gespeichert werden und mit wem und unter welchen Bedingungen sie geteilt werden. Obwohl dieser Begriff in der kürzlich in Kraft getretenen DSGVO nicht verwendet wird, kann die informationelle Selbstbestimmung als Leitprinzip des europäischen Datenschutzes angesehen werden.

3.3.2 TECHNISCHE ERRUNGENSCHAFTEN

Standardisierung, Automatisierung und Prozessoptimierung

Die Blockchain und die darauf durchgeführten Operationen (Transaktionen) folgen einem streng definierten Regelwerk. Diese Regeln werden als festgelegter Standard im (technischen) Protokoll und im Quellcode verankert. Die heterogenen Systeme der Teilnehmer (zum Beispiel auch Unternehmen und Hochschulen) müssen ihre Regeln oder Schnittstellen dergestalt anpassen, dass sie kompatibel mit der dazwischengeschalteten Blockchain sind. Als vermittelndes System setzt ein solches Peer-to-Peer-Netzwerk einen gemeinsamen (Vermittlungs-)Standard. Auf diesem Regelsystem läuft die (Bitcoin-)Blockchain seit 2009 unterbrechungsfrei und ersetzt die Rolle bisheriger Intermediäre durch automatisierte Vorgänge zwischen den Teilnehmern. Eigentum kann transferiert, die Korrektheit nachgewiesen und der abgeschlossene Übertragungsvorgang öffentlich eingesehen werden, sodass beispielsweise Zahlungs- und Liefervorgänge automatisiert verknüpft werden können. Als Folge davon können transparente Transaktions- und Geschäftsabläufe zu optimierten Prozessabläufen führen. Zahlreiche Unternehmen untersuchen seit vielen Jahren die Potenziale der Blockchain bei der Verbesserung der eigenen Geschäftsabläufe (vgl. Epple, 2018).

Beschleunigte Prozesse und Kostensenkung

Als Folge von Dezentralisierung, Automatisierung und Prozessoptimierung werden beschleunigte Geschäftsabläufe erwartet. Während eine SEPA-Überweisung heute noch bis zu mehrere Tage in Anspruch nimmt, können eine Transaktion von Bitcoins und die Verbriefung auf der Blockchain in zehn Minuten stattfinden. Die Interaktion zwischen Vertragsparteien wird von manuellen Teilschritten bei der Verarbeitung

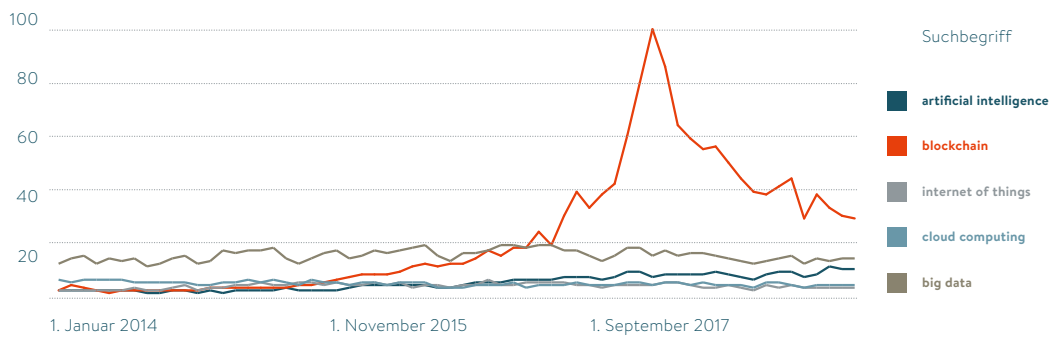
befreit und Transaktionen werden schneller und regelbasierter durchgeführt. Die Vergangenheit hat gezeigt, dass mit einem erhöhten Grad bei der Automatisierung häufig sinkende Kosten für die Prozesse einhergehen. Der Blockchain wird zugeschrieben, dass sie aus wirtschaftlicher Perspektive einen nachhaltigen Beitrag zur Kostensenkung von Transaktionsprozessen liefern kann (vgl. Deubel et al., 2016; Wyman, 2016).

Verändertes Technologiebewusstsein

Kapitel 2 hat dargestellt, dass die Blockchain ein hochkomplexes System verbundener Einzelkomponenten und Konzepte ist (verteilte Systeme, Kryptografie, Hash-Funktionen, spezielle Datenstrukturen, komplexe Regeln, spieltheoretische Elemente usw.), das nicht nur ein technisches Problem löst, sondern auch in der Lage ist, wirtschaftliche und gesellschaftliche Herausforderungen auf neuartige Weise zu meistern. In der Geschäftswelt untersuchen zahlreiche Branchen die Potenziale, die sich aus dieser Technologie ergeben, und auch im Alltag erfährt das Thema eine große Aufmerksamkeit. Die Rollen von Technologie und Selbstverantwortung, aber auch die Rolle bisheriger Intermediäre werden zurzeit nachhaltig überdacht sowie bestehende und bekannte Konzepte zur Diskussion gestellt und mit den Potenzialen, die Blockchains bieten, verglichen. Abbildung 18 zeigt den Suchanfragenverlauf bei Google zum Thema Blockchain.

ABBILDUNG 18: GOOGLE-SUCHANFRAGENVERLAUF ZU POPULÄREN IT-THEMEN

Januar 2014 bis April 2019



Quelle: Google 2019. Abgerufen am 29.05.2019 von https://trends.google.de/trends/explore?date=2014-01-01%20 2019-04-30&geo=DE&q=artificial%20intelligence,blockchain,internet%20of%20things,cloud%20computing,big%20data

3.4 Nachteile der Blockchain

Den Errungenschaften stehen naturgemäß auch nennenswerte Nachteile (über die in Abschnitt 3.2 genannten Beschränkungen hinaus) gegenüber. Die Offenheit der Transaktionen führt zu einer ungewohnten Transparenz, die in Zeiten erhöhter Sensibilisierung für persönliche Daten bei vielen Nutzern Ängste auslösen kann. Datenskandale bei großen Unternehmen (wie der jüngste Skandal bei Facebook (vgl. Spiegel.de, 2018) und die im Mai 2018 in Kraft getretene DSGVO stellen die uneingeschränkte Offenheit von Daten in Frage. Nach einer Umfrage des

Meinungsforschungsinstituts YouGov unter 200 Fach- und Führungskräften sehen 51 Prozent der Befragten dringenden Verbesserungsbedarf beim Schutz vertraulicher Informationen bei der Verwendung der Blockchain (vgl. Soprasteria, 2017). Mit der Bitcoin-Blockchain sind sogar persönliche monetäre Eigentumsverhältnisse offengelegt, nicht nur für Behörden, sondern auch für die anderen Teilnehmer im Netzwerk – der Blick auf das eigene Konto (trotz Pseudonymität) ist jedem gestattet und sorgt zumindest für ein „mulmiges Gefühl". Diese Perspektive beschleunigt die Entwicklung nicht-öffentlicher Blockchains, auf die in Abschnitt 3.7 gesondert eingegangen wird.

VERTRAUEN IN DIE KONSENS- UND ALGORITHMENBASIERTE BLOCKCHAIN

Außer der ungewohnten Offenheit persönlicher Daten wird sich zudem eine neue Form der Selbstverantwortung entwickeln. Mit der Hoheit über den privaten Schlüssel für die persönlichen Daten auf der Blockchain befindet sich nun der Benutzer in einer Situation, in der er selbst nicht nur Herr der eigenen Daten ist, sondern auch die Verantwortung über sein Handeln trägt. Es gibt keine vermittelnde oder verwaltende Instanz mehr, die gegebenenfalls Garantien, Versicherungen oder Hilfeleistungen stellt. Geht der persönliche Schlüssel verloren oder geschehen Flüchtigkeitsfehler bei einer Transaktion, können die Daten nicht mehr bei einem verwaltenden Dienstleister oder einer Behörde eingefordert werden. Mit einem einfachen Gedankenexperiment kann der Leser selbst beurteilen, wie viel Geld er bereit wäre, von seinem realen Bankkonto in Form von Kryptowährungen auf eine Blockchain zu transferieren. Wie groß ist das Vertrauen in die konsens- und algorithmenbasierte „Vertrauensmaschine" Blockchain? Wie ausgeprägt ist das (bisher erarbeitete) technische Verständnis für die Blockchain und der Glaube an die Versprechen dieses komplexen Systems, sodass man bereit ist, vollständig auf die Betreuung eines (gegebenenfalls auch schlichtenden) Intermediärs zu verzichten und seine persönlichen Daten oder sein persönliches Eigentum an einen privaten kryptografischen Schlüssel zu knüpfen?

REINTERMEDIATION

Als Folge der Komplexität, eines geänderten Technologiebewusstseins und offener (oder zumindest unklarer) Rechtsfragen kann eine erneute Reintermediation stattfinden. Öffentliche Blockchains werden nicht-öffentlich aufgesetzt, rein verteilte Peer-to-Peer-Systeme werden doch wieder über hybride Netzwerk-Architekturen quasi-zentralisiert entworfen, um vertrauenswürdige Vermittler in der Transaktionskette dazwischenzuschalten. Ein Beispiel sind Banken, die beispielsweise die Möglichkeiten der Blockchain für interne Zwecke prüfen, aber als Vermittler für den Kunden nach wie vor Dienstleistungen anbieten. Die Blockchain wird somit nicht mehr für die direkte Interaktion zwischen den Teilnehmern benutzt, sondern über den Zwischenschritt einer vermittelnden Instanz. Bisherige Intermediäre werden nicht abgelöst, sondern stärken ihre Position mit der Technologie, durch die sie ursprünglich „überflüssig" werden sollten.

VERLUST VON ARBEITSPLÄTZEN?

Mit den Möglichkeiten der zunehmenden Automatisierung durch standardisiert ablaufende Geschäftsprozesse und die Ablösung von Intermediären geht die Befürchtung vom Verlust von Arbeitsplätzen einher. Ganze Dienstleistungsbranchen zum Beispiel aus der Finanzindustrie, Eigentumsverwalter und Notare sehen ihr Geschäftsmodell gefährdet. Ob die Blockchain als „ultimativer Jobkiller" bezeichnet werden muss, wird kontrovers diskutiert. Der Ökonom Alex Tapscott ist davon überzeugt, dass die Blockchain ganze Berufsbilder reduzieren wird. Wie jede technologische Entwicklung, die zu einer starken Automatisierung und Digitalisierung von Geschäftsbereichen führt, werden Verluste zahlreicher Arbeitsplätze proklamiert, sodass die Blockchain eine gesellschaftliche Herausforderung darstellt (vgl. Tagesanzeiger, 2018). Andere Quellen vertreten die Meinung, dass die Digitalisierung neue Berufsbilder entstehen lässt und so, zumindest absolut gesehen, keine Arbeitsplätze gefährdet sind (vgl. Meier, 2017).

NEUE BERUFSBILDER DURCH DIGITALISIERUNG

3.5 Elementare Anwendungen

Aus der Art und Weise, wie Daten unveränderlich in der Blockchain gespeichert werden, ergeben sich sieben allgemeine elementare Anwendungsfälle, die in verschiedenen Anwendungen verschieden kombiniert werden.

Nachweis einer Existenz

Das Konzept des Bitcoin-Schöpfers Satoshi Nakamoto sah die Blockchain als Mittel zum Nachweis der Existenz von dezidierten Bitcoins und den dazugehörigen Eigentumsverhältnissen. Mittels „Proof Of Existence" kann auch die Existenz neuer wissenschaftlicher Entdeckungen, behördlicher Dokumente, von Design-Entwürfen, Patenten, Markennamen, Lizenzcodes und -bedingungen bewiesen werden. Der Nachweis erfolgt, indem ein elektronisches Dokument zu einem bestimmten Zeitpunkt in einer definierten Form bereits existiert hat. Dabei wird der eindeutige Hash-Wert eines Dokuments errechnet und mit einem Zeitstempel unveränderbar protokolliert. Im Falle eines Konfliktes oder Rechtsstreits kann zu einem späteren Zeitpunkt mit der Neuberechnung und dem Vergleich mit dem unveränderlich hinterlegten Hash-Wert der Beweis erbracht werden, dass das betreffende Dokument zum behaupteten Zeitpunkt bereits existiert hat.[20] Ein solcher Vorgang kann daher mit einem „öffentlichen Notar-Service" verglichen werden.

Nachweis der Nichtexistenz

Ebenso kann der gegenteilige Beweis einer Nichtexistenz geführt werden, dass also kein entsprechender Eintrag zum bisherigen Zeitpunkt vorliegt. Beispielhafte Anwendungen könnten Bußgelder, Mahnungen, Zahlungsverzüge oder Führerscheinpunkte sein. Nach definierten Regeln wird ein solcher Eintrag gehasht und geprüft, ob ein passendes Pendant auf der Blockchain nicht existiert.

Nachweis der Reihenfolge

Eine elementare Eigenschaft zur Überprüfung von Eigentumsverhältnissen ist die sortierungssensitive Speicherung von Eigentumsübergängen. Transaktionen sind in der Blockchain in der Reihenfolge ihrer Eintragungen gespeichert, zudem sind die jeweiligen Zeitstempel hinterlegt. Konkrete Anwendungen könnten die Dokumentation von Prozessabläufen oder die Überwachung von Antragsabläufen sein; insbesondere bei Vorgängen, in denen die Reihenfolge der Anträge oder die Einreichung von Dokumenten ein entscheidendes Element des Prozesses darstellt.

Nachweis des Zeitpunktes

Ähnlich dem Nachweis der Reihenfolge kann der Zeitpunkt, zu dem eine bestimmte (Trans-)Aktion stattgefunden hat, von Bedeutung sein. Bei Einreichungsfristen oder der Nachverfolgung von Zahlungen oder Lieferungen kann der unveränderliche Zeitstempel einer Operation auf der Blockchain genutzt werden, um rückwirkend die Einhaltung von Zeitpunkten zu prüfen.

Nachweis der Identität

In Abschnitt 2.3 wurde gezeigt, wie der Nachweis einer Identität auf der Blockchain erbracht werden kann. An die Identität (von Menschen, Gütern, Tieren oder Gegenständen) sind häufig behördliche oder persönliche Dokumente geknüpft, die mithilfe der Blockchain fälschungssicher hinterlegt und verwaltet werden können.

Nachweis von Eigentum

Ebenfalls in Abschnitt 2.3 wurde dargestellt, wie Eigentum oder Eigentumsverhältnisse mit der Blockchain nachgewiesen werden können. Konkrete Anwendungen für diesen

Fall sind außer digitalem Geld (Kryptowährungen) auch die Verwaltung von Gütern, Lizenzen oder Anteilen zum Beispiel an Immobilien oder Unternehmen.

Nachweis einer Urheberschaft

In Abschnitt 2.5 wurde gezeigt, wie mithilfe der asymmetrischen Kryptografie heutzutage die unbestreitbare Urheberschaft von Nachrichten gewährleistet werden kann. In der Blockchain kann eine Urheberschaft, zum Beispiel eines Textes, über den Zeitstempel und die Identität der einreichenden Person erreicht werden. So können Erstveröffentlichungen, aber auch Änderungen an Inhalten dokumentiert werden.[21] Mit der Nutzung von Werken geht häufig die Vergütung des Rechteinhabers einher, denn insbesondere das rechtswidrige Kopieren und Weiterverbreiten urheberrechtlich geschützter Werke im Internet stellt eine große Herausforderung für die Kreativwirtschaft dar. Die Blockchain kann auch für so einen Anwendungsfall eine mögliche Lösung sein (vgl. Schwirzke, 2016).

3.6 Prominente Blockchain-Projekte und Architekturen

3.6.1 MARKTÜBERBLICK

Die Abschnitte 2.2 und 2.3 haben dargestellt, wie die Technologien der asymmetrischen Verschlüsselung und die Kryptowährung Bitcoin (basierend auf der Blockchain) aus einer fast schon libertären Motivation heraus entwickelt worden sind. Die Unabhängigkeit von staatlichen Organisationen und der Wunsch nach selbstbestimmter Autonomie frei von regulierenden externen Einflüssen haben Zimmermann und Nakamoto nachhaltig in ihren Entwicklungen beeinflusst. Ein libertärer Wunsch nach einer Gesellschaft ohne Institutionen, in der das Vertrauen durch Technologie, Kryptografie und Protokolle geschaffen wird und in der Annahme, dass ein Großteil dieser Gesellschaft ehrlich und nach allgemeingültigen Moralvorstellungen handelt.

↖ SELBSTBESTIMMTE AUTONOMIE

Diese Intention mag entrückt erscheinen, doch bei vielen weiteren Blockchain-Projekten kann der Wunsch nach Autonomie und Selbstbestimmung beobachtet werden. Nach der Finanzkrise 2008 verloren die Geldinstitute massiv an Vertrauen, der Bitcoin (und andere Kryptowährungen) schien eine Alternative zum traditionellen Bankensystem, „wenngleich keine sichere Alternative, dann doch wenigstens eine, die nicht staatlicher Machtpolitik unterliegt“ (Uken, 2017). So lassen sich Non-Profit Blockchain-Projekte, getrieben durch Enthusiasten und technikaffine Akteure der „Maker-Szene“, von kommerziellen und staatlichen Blockchain-Projekten aus dem Bereich e-Government unterscheiden. Diese zunächst eindeutige Kategorisierung zerfasert häufig mit dem Reifegrad eines Projektes, denn oft ergeben sich neue Perspektiven, Anwendungsfälle und Geschäftsmodelle. Die Internetseite Coinmarketcap listet derzeit 2208 Kryptowährungen (vgl. CoinMarketCap, 2019).

↖ E-GOVERNMENT

↖ ICOS – INITIAL COIN OFFERINGS

Schaut man genauer hin, so muss zwischen sogenannten Coins (Münzen) und Tokens (Wertmarken) unterschieden werden (vgl. Giese, 2018). Coins stellen vom Grundverständnis her ein digitales Gegenstück zu Währungsmünzen dar, während Tokens vergleichbar mit Aktien oder Anteilsscheinen sind. Verkauft werden Tokens in „ICOs – Initial Coin Offerings“. Die Abkürzung ICO wurde in Anlehnung an IPO oder „Initial Public Offering“ gewählt. In einem ICO wird eine bestimmte Menge von Tokens zum Verkauf angeboten, sodass die Einnahmen des ICO als Startkapital dienen, um ein Projekt umsetzen zu können – eine Art des Crowdfundings mit digitalen Anteilsscheinen, verbrieft auf der Blockchain.

Coinmarketcap listet mehr als 800 Coins, die fast alle auf der Blockchain (oder zumindest auf der Distributed-Ledger-Technologie) basieren. Weitere DLT über die Blockchain hinaus werden in Abschnitt 3.8 vorgestellt. Während die Kryptowährung Bitcoin versucht, ein unabhängiges, sicheres Bezahlsystem zu etablieren, verfolgen andere Blockchain-basierte Projekte Ziele, die kaum unterschiedlicher sein können. Einige ausgewählte Beispiele sollen im Folgenden – wenngleich jeweils nur kurz – dargestellt werden und die Vielfalt exemplarisch aufzeigen.

TABELLE 5: DIE TOP 20 DER MARKTKAPITALSTÄRKSTEN KRYPTOWÄHRUNGEN

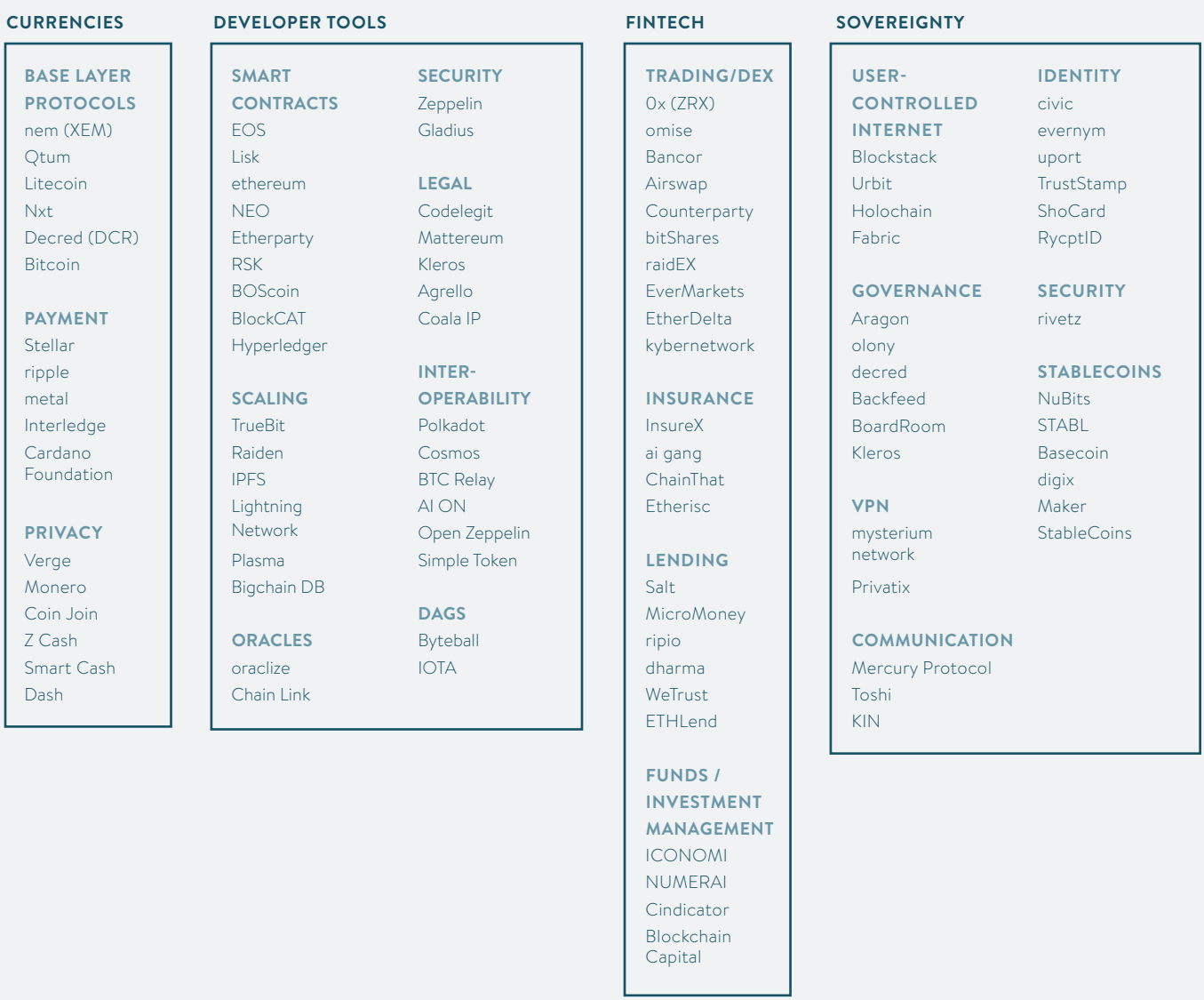
NAME	MARKET CAP IN US-DOLLAR	PRICE IN US-DOLLAR	VOLUME (24H) IN US-DOLLAR	CIRCULATING SUPPLY
BITCOIN	139.623.175.159	7.868,86	19.685.737.658	17.743.762 BTC
ETHEREUM	26.364.324.504	247,84	8.200.820.966	106.376.493 ETH
XRP	17.019.077.511	0,403468	1.478.528.522	42.181.995.112 XRP *
BITCOIN CASH	6.997.059.643	392,59	2.041.113.043	17.822.825 BCH
LITECOIN	6.515.106.768	104,91	3.773.892.796	62.100.951 LTC
EOS	5.871.655.250	6,40	2.594.803.173	917.978.687 EOS *
BINANCE COIN	4.505.793.748	31,92	466.553.589	141.175.490 BNB *
BITCOIN SV	3.522.569.410	197,67	792.319.826	17.820.611 BSV
TETHER	3.221.441.676	1,01	19.468.952.821	3.193.242.376 USDT *
STELLAR	2.379.170.752	0,123071	384.731.426	19.331.689.641 XLM *
TRON	2.231.948.552	0,033471	873.849.966	66.682.072.191 TRX
CARDANO	2.143.759.633	0,082684	108.630.724	25.927.070.538 ADA
MONERO	1.471.458.483	86,43	133.023.631	17.025.414 XMR
DASH	1.303.186.724	147,24	377.679.002	8.850.839 DASH
IOTA	1.193.338.791	0,429331	19.363.868	2.779.530.283 MIOTA *
COSMOS	1.146.413.714	6,01	74.562.420	190.688.439 ATOM *
ETHEREUM CLASSIC	890.275.623	8,02	767.045.863	111.007.705 ETC
NEO	824.018.119	11,68	486.242.777	70.538.831 NEO *
TEZOS	788.354.698	1,19	7.750.702	660.209.075 XTZ *
NEM	746.678.908	0,082964	28.942.450	8.999.999.999 XEM *

Quelle: CoinMarketCap. All Cryptocurrencies. Abgerufen am 06.06.2019 von https://coinmarketcap.com/all/views/all/.

EINE EXEMPLARISCHE KLASSIFIKATION VON ANWENDUNGEN UND ORGANISATIONEN IM BLOCKCHAIN-ÖKOSYSTEM

Josh Nussbaum vom Venture-Capital-Unternehmen Compound hat mit einer detaillierten Übersicht über das Blockchain-Ökosystem versucht (vgl. Nussbaum, 2017), die zahlreichen Akteure und Anwendungen zu klassifizieren. Er unterscheidet hierbei zwischen den Klassen Currencies, Developer Tools, Fintech, Sovereignty, Value Exchange, Shared Data, Authenticity und Others.

ABBILDUNG 19: BLOCKCHAIN PROJECT ECOSYSTEM



Quelle: Nussbaum, 2017

VALUE EXCHANGE

CONTENT MONETIZATION
Streamium
synereo
steem
yours

FILE STORAGE
Filecoin
StoreJ
sia
swarm
MaidSafe
Bigchain DB

DATA
ocean
Enigna
OpenMind
datum
streamr
SynapseAI

COMPUTATION
golem
RNDR
iexec
elastic

MARKETPLACES
Ethlance
district0x
CanYa

MESH NETWORKING
Althea
mmbr
RightMesh
CyberMiles
OpenBazaar
Syscoin
particl

SOCIAL
steemit
KIN
flixxo
PROPS
Akasha

ENERGY
Grid+
PowerLedger
Grid Singularity
Mastodon

VIDEO
Block CDN
Livepeer

SHARED DATA

INTERNET OF THINGS
FOAM
IOTA
Oaken Innovation
Sikorka

SUPPLY CHAIN/ LOGISTICS
Tmining
Walton
Kouvola innovation
Sweetbridge
MONAX
origintrail

ATTRIBUTION
ujo
po.et
JAAK
MyCelia
POEX.io

REPUTATION
ink
Bloom
CHLU
monetha

CURRENT CURATION
userfeeds
curation markets

AUTHENTICITY

DATA
FACTOM
Tierion

TICKETING
GUTS
aventus
Blocktix
TicketChain

OTHER

PREDICTION MARKETS
GNOSIS
augur

VIRTUAL REALITY
Decentraland

STAKING POOLS
1protocol
RocketPool

GAMBLIG
satoshi dice
Fun Fair
Edgeless
Etheroi

GAMING/ E-SPORTS
First Bloo
Huntercoi
Spells of Genesis
gamecredits
Enjin Coin
Bison
Dmarket
Skrilla
unikoin
BitQuest
Dream Team

3.6.2 BITCOIN (BTC) ALS ARCHETYPISCHE BLOCKCHAIN-ANWENDUNG

ARCHITEKTUR EINER BLOCKCHAIN-ANWENDUNG

Mit einer Marktkapitalisierung von über 154 Milliarden US-Dollar und einem täglichen Handelsvolumen von rund 3 Milliarden US-Dollar ist der Bitcoin die stärkste und verbreitetste Kryptowährung. Auf die konzeptionelle und technische Funktionsweise wurde in den vorhergehenden Abschnitten detailliert eingegangen, an dieser Stelle soll eine archetypische Blockchain-Anwendung am Beispiel des Bitcoins gezeigt werden. Die Bitcoin-Blockchain kann mithilfe des Blockchain-Explorers der Internetseite Blockchain.info eingesehen werden. Die Blockchain ist das gemeinsame öffentliche Buchungssystem, auf dem das gesamte Bitcoin-Netzwerk basiert. Sämtliche bestätigten Transaktionen werden in dieser Blockchain gespeichert. Um Transaktionen durchzuführen, also Bitcoins zu senden und zu empfangen, ist ein sogenanntes Wallet (oder auch Kryptowährungs-Wallet) notwendig. Ein solches Wallet kann ebenfalls auf der genannten Internetseite angelegt werden. Bei der Erstellung des Wallets wird eine erste Bitcoin-Adresse (diese fungiert als Public Key) sowie ein Private Key (beides siehe Abschnitt 2.5) generiert, die durch die Wallet verwaltet werden. Mittlerweile existieren verschiedene Varianten von Wallets:

KRYPTOWÄHRUNGS-WALLETS

- Online Wallet (verwaltet durch Web-Dienste wie zum Beispiel Blockchain.info oder bitcoin.de u. v. m.);
- Wallet-Apps für Smartphones (vgl. Bitcoin.de, 2019);
- Wallets für den Desktop (vgl. Bitcoin.de, 2019);
- Hardware-Wallets (vgl. Bitcoin.de, 2019);
- Paper Wallets.

PAPER WALLETS

Paper Wallets stellen eine Besonderheit dar, denn diese zeigen deutlich die Herausforderungen bei der Verwaltung des Private Keys, denn nur wer den Private Key kennt (und behält), ist nachweislich Eigentümer der auf dem Public Key hinterlegten Bitcoins. In Abschnitt 3.4 wurde der Leser dazu angeregt, in einem Gedankenexperiment zu reflektieren, wie viel echtes Geld er bereit wäre, der Blockchain anzuvertrauen. Bei der Verwaltung des Private Keys stellt sich die gleiche Frage: Welchem Internet-Service, welcher Internetseite, welchem App-Hersteller oder welchem Entwickler von Desktop- oder Hardware-Wallets würde der Leser seinen privaten Key anvertrauen? Auch für die Erstellung des Paper Wallets sind aufgrund der Mathematik zur Berechnung des Schlüsselpaares Computerprogramme notwendig. Die Internetseite https://bitcoinpaperWallet.com stellt eine Anleitung zur Verfügung, die aufzeigt, welcher Aufwand betrieben werden muss, um ein sauberes Paper Wallet zu generieren, ohne Gefahr zu laufen, dass während der Erstellung der Keys eine dritte Partei (zum Beispiel der Internetseitenbetreiber, der den Service zur Erstellung eines Paper Wallets anbietet) die Adressen manipuliert.

Mit der Einzahlungsadresse können Bitcoins empfangen werden[22] und mit dem Private Key können Zahlungen an andere Bitcoin-Adressen legitimiert werden. Damit besteht eine einfache Blockchain-Architektur aus folgenden Komponenten:

- Blockchain;
- teilnehmerspezifischer Public Key (als Einzahlungsadresse);
- teilnehmerspezifischer Private Key als Legitimationsschlüssel;
- teilnehmerspezifisches Wallet zur Verwaltung der eigenen Assets (in diesem Fall Bitcoins).

ABBILDUNG 20: PUBLIC (BITCOIN-ADRESSE) UND PRIVATE KEY EINES BITCOIN-PAPER-WALLETS

Typischerweise werden die langen und eingabesensitiven Hash-Adressen der Keys als QR-Codes dargestellt.

Quelle: Acheson, N. (2018). Artikel: How to Make a Paper Bitcoin Wallet, in: Coindesk. Abgerufen am 29.05.2019 von https://www.coindesk.com/information/paper-wallet-tutorial/

3.6.3 ETHEREUM (ETH) UND SMART CONTRACTS

Ethereum (vgl. Buterin, V., et al., 2019) ist ein verteiltes System (siehe Abschnitt 2.1), welches das Anlegen, Verwalten und Ausführen von dezentralen Programmen in einer eigenen Blockchain anbietet. Mit Ethereum soll eine Art dezentraler Computer entstehen, mit dem die klassische Client-Server-Architektur dezentralisiert werden soll. So bezeichnet der amerikanische Software-Entwickler Brian Behlendorf (vgl. Merkel, 2018), einer der führenden Köpfe hinter dem Apache-Web-Server-Projekt, die „Zentralisierung des Internets auf riesigen Serverfarmen als die Ursünde des Internets“, zumal das Internet, so Behlendorf, von Anfang an dezentral gedacht war. Die Ethereum-Plattform soll mit der Dezentralisierung des Internets Mittelsmänner überflüssig machen und dies sowohl beim Hosting von Daten als auch bei der Ausführung von Programmen sowie bei der Überwachung und Erfüllung von zugesagten Eigenschaften (Verträgen).

↖ SMART CONTRACTS

Die Besonderheit von Ethereum sind dabei die Smart Contracts, die aus dem Ethereum-Netzwerk eine dezentrale verteilte Computer-Architektur machen. Smart Contracts sind Programme, die auf dem Ethereum-Netzwerk automatisch ausgeführt werden, sobald vordefinierte Transaktionskonditionen erfüllt sind. Ethereum verwendet dabei die interne Kryptowährung Ether (abgekürzt mit ETH) als Zahlungsmittel für Transaktionsverarbeitungen. Sobald ein im Kontrakt festgelegter Betrag in Ether überwiesen wurde, werden die Smart Contracts automatisch ausgeführt.

Auch mit Blick auf das Internet of Things können Plattformen wie Ethereum einen wertvollen Beitrag leisten. Das Internet der Dinge benötigt eine verbindliche Kommunikation zwischen den beteiligten Geräten. Ein Beispiel für solche Smart Contracts im Kontext der Machine-to-Machine-Kommunikation liefert das deutsche Unternehmen slock.it.[23] Im Geist der Sharing Economy verbindet slock.it Alltagsgegenstände mit der Ethereum-Blockchain und lässt zum Beispiel Schlösser, Waschmaschinen, WLAN-Router und Ähnliches über Smart Contracts auf Zahlungen reagieren. So sind gerade erst neu entstandene und branchenumwälzende Dienste wie Airbnb in ihrer nächsten Entwicklungsstufe sogar gänzlich ohne Menschen beziehungsweise Mittelsmänner möglich. Ethereum (ETH) steht mit einer Marktkapitalisierung von rund 55 Milliarden US-Dollar an Platz zwei der weltweit führenden Kryptowährungen (vgl. CoinMarketCap.com, 2019).

3.6.4 DEZENTRALISIERTE ANWENDUNGEN (DAPPS) UND DEZENTRALISIERTE AUTONOME ORGANISATIONEN (DAOS)

Dezentralisierte Anwendungen (dApps) sind eine neue Form von Onlinesoftware, die so gestaltet ist, dass sie ohne die Kontrolle durch eine einzelne zentrale Instanz im Internet existiert. Während es bei Bitcoin um den dezentralisierten Austausch von Werten geht, verfolgen dezentralisierte Anwendungen das Ziel, Funktionalität jenseits von Transaktionen zu erreichen, bei denen Werte ausgetauscht werden. Mit dem Fortschritt der Blockchain-Technologie entstehen immer mehr Formen von dezentralisierten Apps. In einer vollständig dezentralisierten Welt würden alle Transaktionen mithilfe von Peer-to-Peer-Netzwerken stattfinden und die Vorstellung von zentralen Instanzen wäre nicht existent.

Dezentralisierte Apps können zur Erfüllung ihres Zwecks eine Blockchain nutzen oder sie können selbst eine Blockchain sein. Danach führt die Anwendung selbst keine anwendungsspezifischen Funktionalitäten auf einem Server aus, sondern ihre gesamte Funktionalität wird durch lokale Programme auf Endgeräten verfügbar gemacht. Die Anwendung kann aber auch Server verwenden, die nicht zur App gehören, verbunden mit der Warnung, dass diese nicht Teil der Trusted Computing Base sein müssen. Dies ist zum Beispiel bei Speichersystemen wie Amazon S3 oder Dropbox der Fall, weil die Daten hier Ende-zu-Ende verschlüsselt und verifiziert werden (und den Speichersystemen somit nicht vertraut werden muss).

Dezentralisierte Anwendungen der Ethereum-Blockchain basieren auf Smart Contracts. Sie werden auf der Blockchain und damit auf allen Knoten des Netzwerks parallel ausgeführt. Einen anderen, holistischen und technischen Ansatz zur Implementierung dezentralisierter Anwendungen bietet die Blockstack-Plattform https://blockstack.org (vgl. Ali et al., 2017). Diese etabliert eine eigene Anwendungsschicht auf den bestehenden Protokollen und Infrastrukturen des Internet.

↖ **DECENTRALIZED AUTONOMOUS ORGANIZATIONS (DAO)**

Eine besondere Anwendung von Smart Contracts stellen die sogenannten *Decentralized Autonomous Organizations* (DAO) (vgl. Voshmgir/Kalinov, 2017) dar. Wikipedia erklärt hierzu:

> „Eine Decentralized Autonomous Organization (DAO, deutsch Dezentrale Autonome Organisation) ist eine Organisation, deren Managementstruktur und -regeln digital und unveränderbar durch einen Smart Contract festgeschrieben werden, diese dezentral (z. B. im Ethereum-Netzwerk) ausgeführt werden und daher ohne konventionelle Entscheidungsgremien wie einen Vorstand auskommt. The DAO ist die bekannteste DAO, die bisher auf der Ethereum-Blockchain implementiert wurde. Sie wurde von der Firma slock.it entwickelt und veröffentlicht. Grob zusammengefasst besteht die Aufgabe von The DAO darin, Ether (die Standard-Kryptowährung in Ethereum) durch Verkauf von Stimmberechtigungsanteilen einzunehmen, ein Entscheidungsgremium über die Verwendung des gesammelten Ethers abzuhalten und entsprechend das gesammelte Ether zu überweisen. Es handelt sich also um eine autonome und automatisierte Investmentfirma. The DAO wurde im April 2016 in die Blockchain hochgeladen und durchlief ein Crowdfunding bis zum 28. Mai 2016 (gekauft wurde mit der Kryptowährung Ether). The DAO-Token, die zur Stimmabgabe für die in The DAO getroffenen Entscheidungen berechtigen, können auf diversen Kryptobörsen gehandelt werden.“ (vgl. Wikipedia.org, 2019)

3.6.5 HYPERLEDGER

Hyperledger ist eine von der Linux Foundation im Jahr 2015 gestartete, bereichsübergreifende Open-Source-Initiative zur Förderung branchenübergreifender Blockchain-

Technologien. An diesem weltweiten Gemeinschaftsprojekt nehmen mehr als 130 Unternehmen aus Branchen wie Banken und Finanzen, Internet of Things, Supply-Chain, Fertigung und IT teil.[24] In dieser Initiative werden nicht ein einzelnes Blockchain-Framework beziehungsweise eine einzelne Blockchain-Plattform entwickelt, sondern es werden mehrere Ansätze parallel verfolgt, um den Erfahrungsaustausch zu fördern und Synergien entstehen zu lassen. Die Knoten des Blockchain-Netzwerks bei Hyperledger sind über die teilnehmenden Organisationen verteilt. Nachfolgend wird herausgestellt, dass auf diese Weise besondere Blockchain-Typen entstehen. Die involvierten Organisationen validieren gegenseitig ihre Transaktionen und profitieren als Konsortium davon, dass das Netzwerk und das Vertrauen in die Korrektheit aufrechterhalten bleiben. Die unterschiedlichen Blockchain-Ansätze des Projekts Hyperledger sind derzeit Hyperledger Fabric von IBM,[25] (vgl. Förster, 2017), Hyperledger Burrow,[26] Hyperledger Iroha,[27] Hyperledger Indy[28] und Hyperledger Sawtooth von Intel.[29] Wie mit dem Hyperledger Sawtooth beispielsweise die Abläufe in einer Lebensmittelkette dokumentiert werden können, zeigt die Anwendungsstudie „Seafood Case Study in Supply Chain Traceability Using Blockchain Technology“[30].

3.6.6 WEITERE BRANCHENSPEZIFISCHE BLOCKCHAIN-PROJEKTE

Ripple (XRP)

↖ **„BITCOIN FÜR BANKEN“**

Ripple (XRP) wird häufig als „Bitcoin für Banken“ bezeichnet und soll ein schnelles, skalierbares System sein, mit dem digitale Assets in Echtzeit ausgetauscht werden können. In der Ripple-Blockchain werden – vereinfacht ausgedrückt – Schuldscheine (sogenannte IOU) verwaltet, die Banken oder andere Finanzinstitutionen einander gegenseitig ausstellen. Die gespeicherten Transaktionen sind durch ein Konsensverfahren zwischen unterschiedlichen Ledgern abgedeckt und innerhalb weniger Sekunden unveränderlich über das gesamte Netzwerk gespeichert. Eine der Besonderheiten von Ripple ist es, Transaktionen im Umfang (und der Geschwindigkeit) des VISA-Netzwerks verarbeiten zu können.[31] So gab Spaniens Großbank Santander Anfang 2018 bekannt, für internationale Überweisungen die Blockchain-Technologie des US-Anbieters Ripple verwenden zu wollen (vgl. Louven, 2018). Aktuell weist Ripple eine Marktkapitalisierung von 18 Milliarden US-Dollar auf (vgl. CoinMarketCap.com, 2019).

Zcash (ZEC)

Die Kryptowährung Zcash (ZEC) (vgl. Cryptolist.de, 2019)[32] ermöglicht völlig anonymisierte Transaktionen und verfolgt das Ziel, die Demaskierung von Nutzertransaktionen durch statistische Mustererkennung und Data Mining mithilfe eines kryptografischen Zusatzprotokolls zu verhindern. Der amerikanische Informatiker Matthew Green untersuchte Bitcoin im Hinblick auf die Anonymität der Nutzer und kam zu dem Schluss, dass durch Methoden des Data Mining und der Traffic Analysis Trends in der Masse der Überweisungsvorgänge auf der Bitcoin-Blockchain feststellbar sind und damit zumindest prinzipiell der Zahlungsverkehr für alle Konten eines Nutzers statistisch ermittelbar ist. Als Gegenmaßnahme entwickelte er ein kryptografisches Zusatzprotokoll auf Basis des sogenannten Zero-Knowledge-Proof (vgl. Wikipedia.org, 2019), mit dem Bitcoin-Transaktionen anonymisiert werden können. Zcash hat derzeit eine Marktkapitalisierung von einer halben Milliarde USD (vgl. CoinMarketCap, 2019).

Einsteinium (EMC2)

Beim Einsteinium Coin (EMC2) (vgl. EMC2 Foundation, 2019) handelt es sich um eine Kryptowährung, die sich technisch am Aufbau des Bitcoins orientiert. Mit Einsteinium sollen Wissenschaft und Forschung und insbesondere Projekte, die einen wichtigen Einfluss auf die weitere Entwicklung der Menschheit haben, gefördert werden. Die Investitionen in Forschungsprojekte sollen dabei auf Basis von Community-Entscheidungen

getroffen werden. Durch diesen Spendencharakter erhoffen sich die Entwickler von Einsteinium eine große Akzeptanz für die Tokens bei der wissenschaftlichen Forschungsförderung. Im April 2017 hat sich die Einsteinium-Stiftung als Non-Profit-Organisation eintragen lassen. Sie ist die erste Non-Profit-Organisation, die im Rahmen von Kryptowährungen gegründet wurde. Aktuell hat der Einsteinium-Coin eine Marktkapitalisierung von 27 Millionen US-Dollar.[33]

Steem

Steemit[34] ist eine Social-Media-Plattform, die auf einer Blockchain namens Steem basiert, die nutzergenerierte Inhalte verschiedener Art (Blogs, Tweets, Software, Videos etc.) speichert beziehungsweise verwaltet (vgl. Steem, 2017). Im Fall der Blog-Plattform Steemit ermöglicht die Blockchain-Technologie, die Autoren von Inhalten zu entlohnen, aber auch Benutzer werden für ihre Kommentare zu Inhalten oder das Bewerten von Kommentaren mit einer Kryptowährung belohnt. Die Belohnung für Inhalte und Kommentare erhält zu 75 Prozent der jeweilige Autor und zu 25 Prozent die Bewertenden. Die Auszahlung erfolgt schon sieben Tage nach der Veröffentlichung eines Inhalts. Mit einer Marktkapitalisierung von fast 130 Millionen US-Dollar zählt Steem zu den Top-100-Kryptowährungen (vgl. CoinMarketCap, 2019).

Cardano (ADA)

Cardano (www.cardano.org) ist eine Blockchain-Plattform (ähnlich wie Ethereum), die auf Basis wissenschaftlicher Untersuchungen bisheriger Krypto- und Blockchain-Systeme in den kommenden Jahren eine Krypto-Plattform schaffen möchte, die Performanz, Skalierbarkeit, Sicherheit, Interoperabilität und Funktionsvielfalt in einer einzigen Blockchain vereinigt und die aktuellen Schwierigkeiten bisheriger Blockchain-Anwendungen/-Implementierungen lösen soll. Ein wichtiges Ziel ist es, die Interaktion von Protokollen unterschiedlicher Kryptowährungen untereinander und von Protokollen der äußeren Finanzwelt interagieren lassen zu können. Dabei möchte Cardano einen Mittelweg gehen zwischen der Offenheit gegenüber der öffentlichen Hand und dem Schutz der Privatsphäre der Teilnehmer im Netzwerk und der Dezentralisierung. Cardano verwendet die interne Kryptowährung ADA als Zahlungsmittel für Transaktionen und positioniert sich mit einer Marktkapitalisierung von über 2,3 Milliarden US-Dollar in der Top 10 der Kryptowährungen (vgl. CoinMarketCap, 2019).

↖ **CARDANO (ADA) SOLL ALLE BLOCKCHAIN-VORTEILE VEREINEN**

Enerchain: Dezentraler Energiehandel

Das vom Hamburger Unternehmen Ponton initiierte und mit 43 Energieunternehmen entwickelte Blockchain-Projekt „Enerchain“[35] ist eine dezentrale Handelsplattform, die den Peer-to-Peer-Großhandel von Energie via Blockchain ermöglicht. Aktuelle Anwendungsgebiete umfassen dabei unter anderem den Energiehandel zwischen Händlern zur Vermeidung von Brokern, aber auch Netzauslastung und Regelreserveabrufe in Verteilnetzen durch Übertragungsnetzbetreiber, Verteilnetzbetreiber und Aggregatoren. Im Enerchain-Konzept sollen Teilnehmer ihre Blockchain-Knoten selbst betreiben können, sodass sie im operativen Betrieb nicht auf Dritte angewiesen sind. Darüber hinaus werden im aktuellen Projektrahmen „NEW 4.0“ (Norddeutsche EnergieWende) dezentrale Verfahren für den Handel zwischen Prosumenten und Konsumenten in lokalen Smart Grids untersucht und erforscht.

Cryptofuture: Lieferketten-Management für Lebensmittel

Die Firma CRYPTOFUTURE[36] zeigt in einem Konzept, wie mithilfe der Blockchain eine transparente und nicht veränderbare Protokollierung der Herkunft und des Weges von Lebensmitteln von der Produktion bis zum Konsumenten ermöglicht werden kann. Die Lebensmittel werden mit QR-Codes versehen, die der Endkonsument mit einer Smartphone-App einscannen kann, um so genaue Informationen über den Lebensmittelweg zu erhalten. Das Deutsche Bundesministerium für Wirtschaft und Energie

untersucht derzeit den Themenschwerpunkt Blockchain und hat hierfür Start-ups, Unternehmen und Interessierte eingeladen, ihre Projekte in Form eines Wettbewerbs dem Bundesministerium vorzustellen.[37] Cryptofuture wurde bei rund 600 Einreichungen für diesen Wettbewerb unter die Top 6 gewählt.

Whats2doo: Der Dienstleistungsmarktplatz für die Gig-Economy

Whats2doo[38] ist ein Marktplatz zur Vermittlung von Dienstleistungen im Sinne der sogenannten Gig-Economy (vgl. Wikipedia, 2019), das heißt, auf Basis der Blockchain-Technologie soll hier ein automatisiertes Mitgliederportal für das Buchen jeglicher Art von Diensten und Arbeitskräften entstehen, das im Einklang mit den Anforderungen der Arbeitswelt 4.0 (vgl. Bundesministerium für Arbeit und Soziales, 2016) steht. Dabei sollen von Personenidentifizierungsprozessen, der Verifikation verschiedener Qualifikationen bis hin zur Bezahlung alle Prozessschritte einfacher, schneller, sicherer und günstiger gestaltet werden.

Blockchain in der Versicherungsbranche

↖ **VOLL AUTOMATISIERTE VERSICHERUNGEN**

Der Versicherungskonzern AXA hat mit der Anwendung „Fizzy“ (vgl. AXA, 2017) im Jahre 2017 die erste vollautomatisierte Versicherung auf Blockchain-Basis für Flugverspätungen auf den Markt gebracht. Die Applikation[39] basiert auf der Blockchain und Smart Contracts von Ethereum und arbeitet vom Abschluss bis zur Auszahlung im Schadensfall vollständig automatisiert. Dabei ist das System an eine öffentlich zugängliche Flugverkehrsdatenbank gekoppelt, sodass die definierten Schadensabwicklungsprozesse automatisch ablaufen, wenn sich der gebuchte Flug um mehr als zwei Stunden verspätet, ohne dass der Kunde den Schaden melden muss. Die vereinbarte Entschädigung wird unabhängig von der Ursache innerhalb von sieben Tagen automatisch auf das angegebene Kundenkreditkartenkonto überwiesen.

Schwedisches Grundbuchregister auf Basis der Blockchain

Seit 2016 arbeitet das schwedische Grundbuchamt mit dem Start-up Chromaway in einem gemeinsamen Pilotprojekt zusammen, um das schwedische Grundbuchregister mithilfe einer Blockchain zu modernisieren (vgl. Lantmäteriet et al., 2017). Dabei wird die gesamte Wertschöpfungskette des Immobilienhandels auf der Blockchain abgebildet, von der Hypothek über die Treuhandschaft bis zum Eigentumsübertrag im Grundbuch. Alle Teilnehmer des Prozesses sind dabei identifiziert und ihre Rollen bestätigt (wie zum Beispiel die öffentliche Hand als Akteur im Prozess). Per Smartphone-App werden der Makler und die Bank zur Überprüfung der Daten kontaktiert. Die Beglaubigung erfolgt fälschungssicher auf der Blockchain, als Eingabemedium für die digitalen Unterschriften dient das Smartphone. Die Transaktion des Kaufpreises, also Treuhand und Zahlung, erfolgen wieder auf der Blockchain. Nach überprüfbarem Abschluss wird der Eigentumsübergang digital durchgeführt und der neue Zustand ist in den jeweiligen Apps der Akteure sichtbar. Am Ende sind alle Teilnehmer einer Transaktion, inklusive deren Organisationen und den Vermögenswerten, auf der Blockchain digitalisiert. Primäres Ziel waren die deutliche Reduktion der Bearbeitungszeiten und damit einhergehend signifikante Kosteneinsparungen. So konnte die vollständige Abwicklungszeit für eine Transaktion von vier Monaten auf nur wenige Tage reduziert werden. Die möglichen Einsparungen mit dem Einsatz einer Blockchain wurden von den Projektteilnehmern auf bis zu drei Prozent des Bruttoinlandsproduktes (BIP) geschätzt.

E-Estonia, die Digitalisierungsoffensive von Estland

Im Jahr 2007 war Estland mehrere Wochen lang das Ziel zahlreicher Internetangriffe, die sich gegen staatliche Organe (unter anderem das estnische Parlament und den Staatspräsidenten) sowie gegen Medien und Banken richteten. Diese Angriffe sorgten auch international für große Unruhe, doch für Estland markierten diese

bedrohlichen Vorfälle einen nachhaltigen Wendepunkt auf dem Weg zu einem der am weitesten digitalisierten Staaten der Welt (vgl. Hammersley, 2017). IT-Sicherheit wurde integraler Teil der Landesverteidigung und beschleunigte die Entwicklung zu einer umfassenden digitalen Gesellschaft. Dabei nimmt vor allem die Blockchain eine tragende Rolle ein:

> „After Estonia's experience with the 2007 cyber attacks, scalable blockchain technology was developed to ensure integrity of data stored in government repositories and to protect it data against insider threats." (E-Estonia)

Unter der Bezeichnung „E-Estonia" gilt Estland in Europa heute als Vorreiter des e-Governments. Im Zuge dieser Digitalisierungsoffensive können Estlands Bürgerinnen und Bürger heute 99 Prozent aller Verwaltungsdienste digital nutzen,[40] von der elektronischen Steuererklärung bis hin zum E-Voting. Beispielsweise lagern fast alle Rezeptverschreibungen sicher auf einer Blockchain und werden zwischen Ärzten, Patienten und Apotheken digital kommuniziert (vgl. Einaste, 2018). Die Blockchain ist für Estlands Digitalisierungsstrategie ein wichtiges Werkzeug zur Aufrechterhaltung der Integrität seiner Bürgerdaten (vgl. Sihvart, 2017).

Blockchain zur Dokumentation der Urheberschaft von Forschungsergebnissen

Das im Rahmen des EU-Förderprogramm Horizont 2020 unterstützte Projekt „ResearchProof: An online digital logbook to protect and prove authorship, and to share scientific results"[41] hat mit ResearchProof eine Open-Access-Plattform entwickelt, auf der Ergebnisse (und Zwischenergebnisse) aus Forschungsprojekten oder wissenschaftlichen Arbeiten veröffentlicht werden können und auf einer Blockchain die Urheberschaft nachweislich dokumentiert ist (siehe Abschnitt 3.5, Nachweis einer Urheberschaft). Das Projekt kommt zu dem Ergebnis:

> „The expected outcome of the project is to successfully execute the market validation and demonstrate that the value of sharing scientific results at all phases of the research cycle. The daily logbook will enable easy recording and tracking of daily results from any one researcher or research group. ResearchProof encourages open access to data and will promote publication of negative and intermediate results giving value to all results. The ResearchProof development will boost economic growth and create jobs within Innovaetica." (www.fabiodisconzi.com, 2019)

Blockchain sticht in See: Digitalisierung von weltweiten Lieferketten

Die Firma Maersk, das weltweit führende Unternehmen im Bereich Container-Logistik, hat in einer internen Untersuchung herausgefunden, dass beispielsweise eine Lieferung von gekühlten Produkten von Ostafrika nach Europa eine Kette von fast 30 Personen und Organisationen passieren kann und damit mehr als 200 unterschiedliche und teils fehleranfällige Interaktionen und Kommunikationsschritte unter allen Beteiligten, in vielen Teilschritten noch auf Papier, notwendig sind. Gemeinsam mit IBM hat Maersk ein Joint Venture (vgl. Moller, 2018) gegründet, um unter anderem die Blockchain als Instrument einzusetzen, um Transporte für alle Beteiligten einer Lieferkette End-to-End sichtbar zu machen und den jeweils berechtigten Partnern den Zugriff auf vertrauenswürdige Daten in Echtzeit zu ermöglichen. Es erlaubt vor allem, dass die unterschiedlichen Handelspartner eine „single version of truth" (Konsens) auf eine Transaktion bekommen, also eine einheitliche Version dessen, was von allen Beteiligten als korrekt betrachtet wird. Die Tests mit verschiedenen Partnern wie Hafengesellschaften, Unternehmen oder Zollbehörden haben erfolgreich gezeigt, wie eine solche Plattform einen Transport für alle Beteiligten einer Lieferkette end-to-end sichtbar machen und gleichzeitig benötigte Dokumente digitalisiert und die Abfertigung automatisiert werden kann.

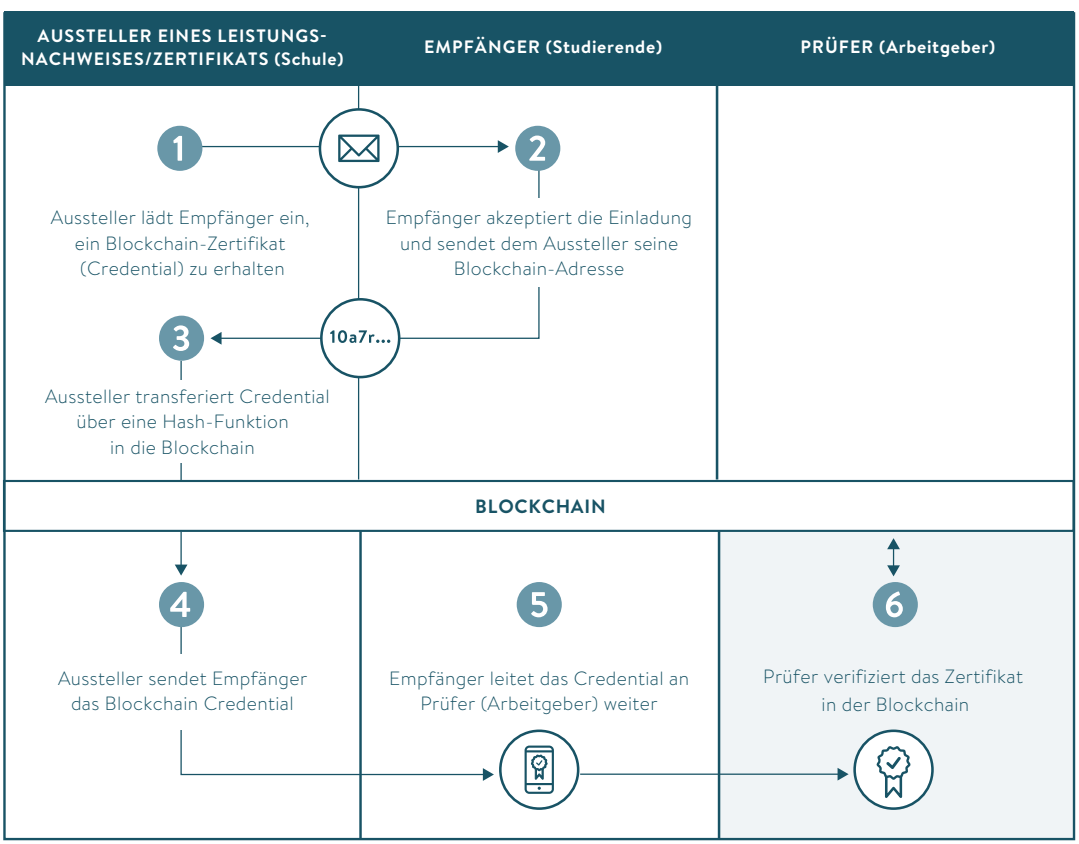
R3-Konsortium

R3[42] wurde 2015 von den Banken Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street und UBS gegründet. Mittlerweile haben sich über 80 Banken und mehr als 200 Firmen im Konsortium R3 zusammengeschlossen, um eine eigene Open-Source-Version der Blockchain namens Corda zu entwickeln. Corda ist eine Plattform für die betriebliche Anwendung der Blockchain für die Finanzindustrie und den Handel. Gemeinsam mit den Mitgliedern des Konsortiums werden Proofs of Concept entwickelt, um Distributed-Ledger-Applikationen kommerziell zu nutzen.

Blockcerts

Blockcerts[43] ist ein offener Standard und eine Plattform für digitale, Blockchain-basierte Datenverwaltung. Die Software besteht aus Open-Source-Bibliotheken, verschiedenen Werkzeugen und Smartphone-Apps (vergleichbar mit den Wallets bei Kryptowährungen). Mit diesem dezentralen und auf den Nutzer ausgerichteten Ökosystem sollen Validierungsprozesse ohne Drittparteien sowie dem Benutzer die Selbstverwaltung von Identitäten und Dokumenten ermöglicht werden. Als Anwendungsbeispiele können die Verwaltung von Lebensläufen, akademischen Nachweisen und sonstigen Leistungs- bzw. Bildungsnachweisen genannt werden.

ABBILDUNG 21: ARCHITEKTUR EINER BLOCKCERTS-ANWENDUNG



Quelle: Introduction, in: Blockcerts. Abgerufen am 29.05.2019 von https://www.blockcerts.org/guide/

3.7 Soziotechnische Typen von Blockchains

Zu Beginn dieses Kapitels wurde gezeigt, dass die Blockchain zahlreiche Widersprüche zu lösen hat und komplementäre Anforderungen teilweise nur durch Kompromisse erfüllt werden können. Aus diesen Widersprüchen speisen sich verschiedene Unterscheidungen von Idealtypen der soziotechnischen Architektur und Implementierung von Blockchains. So führt das Spannungsverhältnis von Vertraulichkeit und Transparenz zu einer Unterscheidung von öffentlichen und privaten Blockchains (public/private), das Spannungsverhältnis von Sicherheit und Geschwindigkeit zu der Unterscheidung von genehmigungsfreien und genehmigungspflichtigen Blockchains (permissionless/permissioned). Das Spannungsverhältnis von in der Regel durch Individuen und wirtschaftliche Anreize getriebenen Innovation und Gemeinwohl liegt der Unterscheidung von offenen und geschlossenen Blockchain-Anwendungen (gegebenenfalls mit proprietären Elementen) zugrunde.

Es muss darauf hingewiesen werden, dass die Wahl des Blockchain-Typs Auswirkungen auf zentrale Aspekte der Blockchain hat. Kapitel 1.1 hat gezeigt, dass in einem rein verteilten Peer-to-Peer-System das Prinzip „Gleicher unter Gleichen“ gilt. Werden die Eigenschaften private oder permissioned oder proprietary gewählt, kann bei der dadurch entstehenden Blockchain nicht mehr von einem rein verteilten P2P-System gesprochen werden. Werden nur ausgewählten Teilnehmern exklusive Schreib- und Überprüfrechte gewährt, so verliert das System ebenfalls Aspekte seiner verteilten Natur. Es entstehen Knoten im System, die eine exponierte Rolle und damit eine besondere Verantwortung haben. Führt der Ausfall eines solchen Knotens zu Beeinträchtigungen des Systems, so ist die Architektur gemäß Kapitel 1.1 eher als Hybridsystem mit hierarchischen Elementen zu betrachten, wenn nicht sogar als System mit verborgener Zentralität.

Es muss für den jeweiligen Anwendungsfall sorgfältig abgewogen werden, welcher Blockchain-Typ die richtige Wahl ist, um die Vorteile und Errungenschaften der Blockchain tatsächlich nutzen zu können und gleichzeitig die Nachteile zu vermeiden.

3.7.1 OFFENE, GESCHLOSSENE UND HYBRIDE BLOCKCHAIN-ARCHITEKTUREN

Blockchain-Implementierungen unterscheiden sich erheblich zwischen verschiedenen Anbietern, insbesondere hinsichtlich der folgenden Kriterien:

↖ BEWERTUNGSKRITERIEN FÜR BLOCKCHAIN

- *Governance:* Blockchains können entweder eine dezentrale Governance haben, bei der alle Nutzer das gleiche Mitspracherecht bei den Regeln genießen, denen die Blockchain unterliegt, oder eine zentrale Governance, bei der eine Person oder eine kleine Gruppe von Personen die Regeln festlegen, die für alle anderen Nutzer der Blockchain gelten.
- *Datenportabilität:* Einige Blockchains ermöglichen es dem Nutzer, seine Daten durch die Verwendung von Interoperabilitätsstandards in andere Blockchains zu übertragen, während andere Ketten keine für die Interoperabilität notwendigen Informationen bereitstellen.
- *Verifizierung:* Einige Blockchains bieten einen offenen Zugang, um die in ihnen enthaltenen Daten zu lesen und damit Transaktionen zu verifizieren, während andere erst nach Autorisierung den Zugriff erlauben.
- *Zugriff auf Wallets:* Einige Blockchains erlauben es den Nutzern, eine Kopie der gesamten Blockchain direkt auf ihrem eigenen Gerät zu speichern, zusammen mit den Daten, die ihnen den Zugriff auf ihre Tokens ermöglichen. Andere Plattformen erlauben den Zugriff auf die Tokens und die Blockchain lediglich über dazwischengeschaltete (meist Cloud-basierte) Software.

» *Open Source:* Viele Blockchains legen ihre Software in ihrer Gesamtheit offen, während einige andere einen Teil oder den gesamten Code als proprietäres, vertrauliches geistiges Eigentum für sich behalten.

Diese Aspekte von Blockchain finden sich in den Typen von *offenen* und *geschlossenen* (auch proprietären) Blockchain-Architekturen wieder, wie im Folgenden dargestellt:

ABBILDUNG 22: VERGLEICH VON OFFENEN UND GESCHLOSSENEN BLOCKCHAIN-ARCHITEKTUREN

Quelle: Camilleri, A. (2018). Comparison of Open vs Closed Blockchain Architectures. Abgerufen am 29.05.2019 von https://doi.org/10.6084/m9.figshare.6981884.v1

Die archetypische offene Blockchain ist die Bitcoin-Blockchain, während private Blockchains, die von Unternehmen für das Supply-Chain-Management verwendet werden, Beispiele für vollständig geschlossene Blockchains sind. Viele börsennotierte Blockchain-Unternehmen verwenden Hybrid-Blockchains, die einige offene und geschlossene Merkmale miteinander kombinieren, wobei sich jede Hybrid-Blockchain durch eine individuelle Kombination von Elementen dieser beiden Idealtypen auszeichnet.

3.7.2 ÖFFENTLICHE UND PRIVATE BLOCKCHAINS

Die Transaktionshistorie ist auf der Blockchain völlig offen und transparent einsehbar gespeichert. Sie ist konzeptionell und notwendigerweise – zum Beispiel zur Vermeidung des Double-Spending-Problems – als öffentliches Hauptbuch angelegt. Abschnitt 3.4 hat gezeigt, dass diese Offenheit in bestimmen Fällen jedoch unerwünscht ist. Im Großen und Ganzen lassen sich hinsichtlich des Konfliktes zwischen Vertraulichkeit und Transparenz im Betrieb und Zugang zwei idealtypische Formen des Einsatzes von Blockchain-Lösungen unterscheiden, die erhebliche Unterschiede in Architektur und Governance aufweisen. Diese Unterscheidung ist verwandt, aber nicht identisch mit der bereits vorgenommenen Unterscheidung in offene und geschlossene Blockchains, die auf die technische Architektur und den technischen Zugang fokussiert.

Öffentliche Blockchains (public blockchains) sind für jedermann zum Herunterladen, Ausführen und Tätigen offen. Sie können von allen Nutzern offen eingesehen werden und jeder kann neue Transaktionen einfügen. Es bestehen volle Lese- und Schreibrechte für alle Benutzer. Öffentlich betriebene Blockchains sind verwandt,

aber nicht zu verwechseln mit offenen Blockchains: Öffentlich betriebene Blockchains können nach der bereits vorgenommenen Unterscheidung sowohl offen als auch geschlossen – oder hybrid – implementiert sein. Öffentlich betriebene Blockchains beruhen auf öffentlicher Konsensfindung, um Entscheidungen zu treffen, und können auf Millionen von Rechnern betrieben werden. Öffentlich betriebene Blockchains erzeugen also ein Maximum an Unveränderlichkeit, Dezentralisierung und Transparenz – allerdings auf Kosten von hoher Ineffizienz in Form von hohen Speicherkosten, hohem Stromverbrauch sowie niedriger Transaktionsgeschwindigkeit und niedrigem Durchsatz.

Demgegenüber sind private Blockchains nur auf Einladung zugänglich und funktionieren nach einer Reihe von Regeln, die von den Einladenden aufgestellt wurden. Eine solche Blockchain kann von einer kleinen Anzahl von Vertragsparteien genutzt werden, um ausschließlich untereinander zu handeln, oder sie kann jedem offen stehen zur Ausführung von Transaktionen, wobei die Kontrolle über die Blockchain und gegebenenfalls Validierung der Transaktionen einer kleinen ausgewählten Gruppe vorbehalten bleibt. Effektiv reduziert eine privat betriebene Blockchain die Unveränderlichkeit und Transparenz der Kette, ist hochgradig zentralisiert (und bietet dabei immer noch mehr Vorteile als eine herkömmliche Datenbank) – allerdings auch kleiner und spezialisierter, mit hoher Effizienz, hohem Durchsatz und hoher Transaktionsgeschwindigkeit und dadurch geringeren Kosten und geringerem Ressourceneinsatz.

Das Modell einer von einem Konsortium betriebenen Blockchain ist eine Mischung aus den Typen öffentlich und privat betriebener Blockchains. Eine Konsortialblockchain ist zunächst eine nicht-öffentlich von einem Konsortium betriebene Blockchain, an der nur ein ausgewählter Kreis an Personen und Organisationen teilnimmt, die zugleich Mitglieder des Konsortiums sind. Gleichzeitig verfügen alle Teilnehmer über gleiche oder ähnliche Stimmrechte beziehungsweise werden die Entscheidungen im Konsens getroffen. Aus Governance-Perspektive bleibt somit der dezentrale Charakter einer öffentlich betriebenen Blockchain erhalten. Bezogen auf die Unveränderlichkeit, Transparenz und den Ressourceneinsatz liegen Konsortialblockchains zwischen den Merkmalen privat und öffentlich betriebener Blockchains.

3.7.3 GENEHMIGUNGSFREIE UND GENEHMIGUNGSPFLICHTIGE BLOCKCHAINS (PERMISSIONLESS BLOCKCHAINS VERSUS PERMISSIONED BLOCKCHAINS)

Bezüglich der Widersprüche bei Geschwindigkeit versus Sicherheit ist vor allem die Frage wichtig, wem Schreibrechte gewährt werden. Darf jeder Teilnehmer schreiben, so muss mit dem bekannten, rechenintensiven Arbeitsnachweis sichergestellt werden, dass Manipulationen durch den Schreibenden vom Netzwerk erkannt werden. Hat nur eine ausgewählte Gruppe von Teilnehmern Schreibrechte, also das Recht, neue Transaktionen anzuhängen, steigt die Verarbeitungsgeschwindigkeit und damit die Anzahl der Transaktionen pro Sekunde. Abschnitt 2.9 hat dargestellt, wie die Schwierigkeit dynamisch an die Rechenleistung des Netzwerks angepasst wird, um die Aufwände für die Arbeitsnachweise („Proof of Work“) hoch zu halten.

Hinsichtlich der Schreibrechte können wieder zwei Typen von Blockchains unterschieden werden:

» *Genehmigungsfreie Blockchains* (permissionless blockchains) ermöglichen jedem Teilnehmer, Transaktionen einzufügen und andere Transaktionen auf Korrektheit zu überprüfen.
» *Genehmigungspflichtige Blockchains* (permissioned blockchains) erlauben nur einer

bestimmten Gruppe von Teilnehmern den Schreibzugriff auf die Blockchain, also das Hinzufügen und Überprüfen von Transaktionen. Die Besonderheit besteht darin, dass die Vertrauenswürdigkeit der Teilnehmer dieser Gruppe bekannt ist und Nutzer mit Schreibgenehmigung häufig im Rahmen eines Beitrittsverfahrens überprüft werden.

Die bisher beschriebene Bitcoin-Blockchain kann in dieses Schema als öffentlich und genehmigungsfrei (und zugleich als offen) eingeordnet werden, sie gilt als die am wenigsten beschränkte Variante, ist aber zugleich transparent und langsam. Die restriktivste Variante, privat und genehmigungspflichtig (oft geschlossen/proprietär), wird häufig im kommerziellen Umfeld eingesetzt, da sie die höchste Verarbeitungsgeschwindigkeit ermöglicht und zugleich sensible Daten vor der Öffentlichkeit verborgen hält. Die in Kapitel 2.6 gezeigten Ansätze der Hyperledger-Initiative stellen private genehmigungspflichtige Blockchains dar.

3.8 Abwandlungen, Weiterentwicklungen, Alternativen

3.8.1 FORKS VON BLOCKCHAINS

Abschnitt 3.6 hat dargestellt, dass mehr als 1.600 Kryptowährungen existieren (Tokens und Coins zusammengenommen) und viele dieser Blockchain-Implementierungen stellen tatsächlich Derivate voneinander dar. Die Ursache hierfür besteht darin, dass die meisten dieser Implementierungen Open Source (vgl. Github, 2019) sind. Da Open-Source-Software naturgemäß frei zugänglich ist, darf jeder diese Software auch nach seinen eigenen Vorstellungen modifizieren. Dieser Vorgang wird als Fork („Abspaltung“) bezeichnet, also die Weiterentwicklung von Open-Source-Software auf einem parallelen Zweig. Dieses Modifizieren ist erwünschter Bestandteil des Open-Source-Gedankens und soll die Entstehung qualitativ hochwertiger, evolvierter Software ermöglichen und die Vielfalt fördern. Abschnitt 3.1 hat als eine der Eigenschaften die Unveränderlichkeit der Blockchain herausgearbeitet, was zunächst widersprüchlich anmutet, da der Quellcode zum Beispiel von Bitcoin für jedermann offen und frei umprogrammierbar ist. Beschränkungen, wie zum Beispiel die mangelnde Skalierbarkeit oder Eigenschaften wie die Blockgröße, die verwendeten Hash-Funktionen, bessere Datenstrukturen und vieles mehr, können leicht umprogrammiert und zu einer neuen, besseren Blockchain führen.

In der Praxis sieht eine solche Fork folgendermaßen aus:

» Ausgehend von einer allgemein anerkannten Version (zum Beispiel der Bitcoin-Blockchain) wünschen sich die Nutzer des Netzwerks neue Funktionen oder das Beheben bisheriger Beschränkungen;
» ein Entwickler (oder eine Gruppe von Entwicklern) modifiziert den Quellcode der derzeitigen (Bitcoin-)Software und stellt sie anderen Nutzern zur Verfügung;
» auf diese Weise entsteht ein neues Netzwerk mit einer neuen Blockchain – allerdings in zwei Versionen, bei denen die Nutzer entscheiden können, welche der Versionen sie künftig nutzen.

Diese Entscheidung ist eine Entweder-Oder-Entscheidung, da alle Knoten im Netzwerk die gleiche oder zumindest eine kompatible Version verwenden müssen (in Abschnitt 2.6 wurde beschrieben, dass in den Metadaten des Block-Headers unter anderem auch die Version gespeichert ist). Hinsichtlich der Kompatibilität gibt es zwei Arten von Forks.

Eine *Soft Fork* zeichnet sich durch Abwärtskompatibilität zur bestehenden Version aus. Dies führt dazu, dass zwei Versionen gleichzeitig im Netzwerk betrieben werden und es Netzwerkknoten gibt, die noch die alte Version einsetzen, während immer mehr Knoten die neue Version verwenden. Ist eine Mehrheit im Netzwerk erreicht, verständigen sich in der Regel alle Knoten auf die neuen (Versions-)Blöcke. Somit arbeiten eine Zeit lang alte Knoten (also jene mit der alten Version) und neue Knoten parallel zusammen in einem Netzwerk. Die Besonderheit besteht darin, dass aufgrund der Abwärtskompatibilität die bisherige Blockchain weiter verwendet werden kann. Dies führt allerdings auch zu der Einschränkung, dass fundamentale Änderungen nicht implementiert werden können, zum Beispiel das Ändern einer kryptografischen Hash-Funktion.

Die zweite Variante einer Fork (Abspaltung) stellen *Hard Forks* dar, diese sind nicht abwärtskompatibel und bringen große Herausforderungen mit sich. Knoten müssen ihre Software zwingend aktualisieren, um weiterhin Teilnehmer des Netzwerks sein zu können, und deswegen benötigt die neue Version einen breiten Konsens bei den Teilnehmern. Die Inkompatibilität der Versionen führt dazu, dass das Netzwerk (die Teilnehmer) gesplittet wird in einen Teil, der die Änderungen akzeptiert und am neuen Netzwerk partizipiert, und einer Nutzergruppe, die sich gegen die Änderungen ausspricht. Die Blockchain wird ab diesem Zeitpunkt aufgeteilt (dupliziert) und es existieren nunmehr zwei verschiedene, zueinander inkompatible Versionen der Ursprungs-Blockchain. Alte und neue Knoten beschreiten nun getrennte Pfade.

↖
„THE DAO"-HACK

Das bekannteste Beispiel einer solchen Hard Fork, bei der unter den Nutzern kein Konsens gefunden werden konnte und daher zwei Blockchains entstanden, die bis heute koexistieren, war die Konsequenz aus dem „The DAO"-Hack im Jahr 2016 (vgl. Biederbeck, 2016). Damals entdeckte ein unbekannter Hacker eine Sicherheitslücke (je nach Sichtweise nutzte der Hacker auch nur einen Fehler in der Logik der Smart Contracts aus) und erbeutete DAO-Tokens im Wert von mehr als 50 Millionen US-Dollar. The DAO basierte auf Ethereum und die Community sowie die Ethereum-Entwickler diskutierten über viele Wochen intensiv darüber, den Transfer der gehackten Tokens rückgängig zu machen. Die Idee kam auf, eine Blockchain neu zu berechnen (hierzu ist ein enormer Rechenaufwand notwendig), die den Transfer der erbeuteten Tokens auf den Account des Hackers nicht enthielt, dies entsprach aber einer Hard Fork und hätte den Konsens der Community benötigt. „Hardliner" der Community verweigerten jedoch dieses Update, denn sie sahen in dieser Lösung eine Verletzung der Ideale von Ethereum. Aus Protest blieben sie bei der alten Blockchain und tauften diese Ethereum Classic, während die Haupt-Blockchain von Ethereum den Hack nicht mehr enthielt und so zwei bis heute existierende Versionen entstanden.

↖
ETHEREUM VS. ETHEREUM CLASSIC

Auch von Bitcoin existieren mittlerweile mehrere Varianten, die aus Hard Forks entstanden; zu den bekanntesten Varianten zählen: Bitcoin Cash (bei dem zum Beispiel die Blockgröße von 1 Megabyte auf 8 Megabyte erhöht wurde und damit die Verarbeitungsgeschwindigkeit von Transaktionen steigt), Bitcoin Gold (hier wurde unter anderem der Hash-Algorithmus von SHA256 auf Equihash geändert, um nicht mehr, wie Bitcoin, auf hochoptimierte ASICs angewiesen zu sein), Bitcoin Private (basiert zum Beispiel auf zk-SNARK (vgl. Z.Cash, 2019) zur Erhöhung der Privatsphäre). Die indische Economic Times prognostiziert für 2018 mehr als 50 Bitcoin-Forks (vgl. Kharif, 2018) und tatsächlich stellt ein Großteil der Kryptowährungen Abspaltungen bekannter Implementierungen dar, die jeweils ihren Fokus auf andere Eigenschaften legen.

Die Nachteile oder Beschränkungen der (Ur-)Blockchain werden also sukzessive behoben und anwendungsspezifisch Detaillösungen erarbeitet, sei es hinsichtlich

Datenschutz und Privatsphäre, Skalierung, Transaktionsgeschwindigkeit oder der Art und Weise, wie Konsens geschaffen wird.

3.8.2 KONSENSVERFAHREN

Proof of Work (PoW)

Abschnitt 2.8 hat dargestellt, wie das für Bitcoin bewusst gewählte Konsensverfahren „Proof of Work" (PoW) dazu eingesetzt wird, die Integrität der Blockchain aufrechtzuerhalten und die Teilnehmer über spieltheoretische Ansätze als Akteure und Kontrolleure in eine Wettbewerbssituation zu bringen. Dieses rechen- und ressourcenintensive Verfahren wird häufig als Nachteil und „enorme Ressourcenverschwendung" bezeichnet, ist aber konzeptionelle Grundlage von Bitcoin.

Andere Implementierungen (Forks) verwenden alternative Konsensverfahren mit anderer Schwerpunktsetzung. Exemplarisch werden weitere populäre Konsensverfahren kurz dargestellt.

Proof of Stake (PoS)

Proof of Stake (vgl. Github, 2019), auf Deutsch etwa „Anteilsnachweis", bezeichnet ein weiteres Verfahren, mit dem in einem Blockchain-Netzwerk Konsens darüber erzielt wird, welcher Teilnehmer den nächsten Block für die Blockchain erzeugen darf. Hierbei wird eine gewichtete Zufallsauswahl verwendet, bei der die Gewichte der Teilnehmer aus dem Vermögen (Stake) und/oder der Teilnahmedauer am Netzwerk ermittelt werden. So wird die Stimmgewalt der Teilnehmer nicht durch die Rechenleistung, sondern durch die Höhe des Vermögens definiert unter der Annahme, dass jene Teilnehmer, die viel besitzen, auch daran interessiert sind, dass das Netzwerk weiterhin vertrauenswürdig ist. Verliert das Netzwerk an Vertrauen/Glaubwürdigkeit, verlöre es an Relevanz und damit an Wert. Zudem wird das Stapeln oder Anhäufen von Anteilen dadurch motiviert, dass Eigentümer dieser Währung Zinsen erhalten (üblicherweise 1 bis 5 Prozent pro Jahr). Populäre Kryptowährungen, die dieses Konsensverfahren einsetzen, sind DASH, NEO oder in einer der kommenden Ausbaustufen auch Ethereum (Casper, vgl. Zamfir, 2017). Es ist offensichtlich, dass mit dem Stapeln der Anteile die Gefahr einer Quasi-Zentralisierung einhergeht. Es sind auch Kombinationen der Konsensverfahren Proof of Work und Proof of Stake denkbar, etwa indem die Schwierigkeit zur Lösungen des Hash-Puzzles bei PoW antiproportional an die Höhe des Vermögens eines Teilnehmers gekoppelt wird.

Proof of Capacity (PoC)

Proof of Capacity, auch Proof of Space (vgl. Dziembowski et al., 2015) oder „Kapazitätsnachweis" genannt, setzt als Konsensverfahren anstelle von Rechenleistung auf Speichergröße. Das Mining-Prinzip des PoC sieht vor, dass Miner einmalig Datensegmente generieren und auf ihrer Festplatte speichern, wo sie dann für weitere, künftige Blöcke genutzt werden können. Da es auch hier Varianten gibt, hilft eine Analogie abseits der Blockchain, das Konzept dahinter leichter zu verstehen: Um beispielsweise E-Mail-Spam zu verhindern, könnte ein Mail-Konto-Anbieter im Gegenzug vom Benutzer ein gewisses Kontingent an Festplattenspeicher einfordern. Für jedes Konto wird dieser Speicher geprüft (beispielsweise indem der Benutzer aufgefordert wird, probeweise eine große Datei herunterzuladen). Was für einen normalen E-Mail-Nutzer eine geringe Hürde darstellt, wird für Massenversender von E-Mails zu einem Problem, da es den Massenversand von Spam-Mails unrentabel macht. Die 2014 gegründete Kryptowährung Burst-Coin (vgl. burst-coin.org) verwendet dieses Konsensverfahren. Aktuell weist das Burst-Coin-Netzwerk eine Größe von fast 230.000 Terabyte, also 230 Petabyte auf.[44]

Proof of Activity (PoA)

Das Konsensverfahren Proof of Activity (vgl. Bentov/Lee/Mizrahi/Rosenfeld, 2014) stellt eine Kombination aus den PoW und PoS dar und vereint den Arbeitsnachweis mit dem Besitznachweis. Zunächst wird per Proof of Work ein gültiger Hash-Wert für den aktuellen Block mit vorgegebener Komplexität gesucht. Der Block gilt dann als abgeschlossen, wenn eine vordefinierte Anzahl zufälliger Besitzer den Block mit ihrem Private Key signiert hat. Die Teilnehmer für die Signierung werden dabei nach dem Proof-of-Stake-Verfahren ausgewählt. Abschließend wird die Belohnung für die Blockgenerierung zwischen den Proof-of-Work-Minern und den signierenden Teilnehmern aufgeteilt. Damit kann die Schwierigkeit niedriger gehalten werden und durch die Mehrfachprüfung eines Blocks wird die Blockchain zusätzlich vor Manipulationen geschützt. Eine Kryptowährung, die auf einem solchen Konsensverfahren basiert, ist Decred.[45]

Proof of Correctness (PoC)

Das Proof-of-Correctness-Konsensprotokoll ist vor allem als der „Ripple- (siehe Abschnitt 3.6, Ripple) Protocol-Consensus-Algorithmus (RPCA)“ (vgl. Schwartz/Youngs/Britto, 2014) bekannt. So basierten die bisher genannten Konsensverfahren darauf, dass die Teilnehmer einen neuen Block erzeugen und dieser (im Netz verteilt) an die Blockchain angehängt wird. Bis die Synchronisation der Blockchain-Instanzen abgeschlossen ist, vergeht eine gewisse Zeit, insgesamt entsteht also ein Zeitbedarf aus Blockbildung und -verteilung. Anders geht der RPCA vor, denn hier werden die zu überprüfenden Transaktionen als Kandidaten bezeichnet, die den Knoten des Netzwerks als Kandidatenbündel (Candidate Sets) zur Verfügung stehen. Der Konsensmechanismus soll nun Einigung über eine gemeinsame Teilmenge der Kandidaten herstellen, was asynchron und iterativ geschehen kann. Die Besonderheit besteht nun darin, dass die Knoten Vorschläge für Kandidaten einreichen und die Korrektheit dieser Transaktionen prüfen, wenn sie im eigenen Kandidatenbündel enthalten sind. Dieser Effekt schaukelt sich hoch und es wird ein gemeinsamer Konsens über validierte Kandidaten geschaffen, die ab einer bestimmten Menge von positiven Vergleichen der Blockchain hinzugefügt werden (vgl. Roßbach, 2016).

Weitere Konsensverfahren

Als weitere Konsensverfahren sind zu nennen: Proof of Burn zum Beispiel bei der Kryptowährung Slimcoin (vgl. Slimcoin, 2014), Proof of Authority verwendet auf der VeChain-Blockchain,[46] Proof of Importance von NEM[47] oder auch der von Intel entwickelte Proof of Elapsed Time (PoET) (vgl. Hyperledger Sawtooth, 2019).

3.8.3 WEITERE ENTWICKLUNGSPFADE DER BLOCKCHAIN-TECHNOLOGIE

Koentwicklung von Hash-Funktionen und Hash-Hardware

Die Abschnitte 2.5, 3.2 und 3.6 haben gezeigt, dass die Auswahl geeigneter Hash-Funktionen ein wichtiges Element für die Austarierung der Blockchain ist. Je nach Blockchain-Implementierung kommen unterschiedliche Hash-Funktionen an den verschiedenen Stellen der Architektur parallel zum Einsatz. So existieren Blockchains, bei denen das Hash-Puzzle bewusst rechenaufwendig gehalten und der Einsatz von ASICs begünstigt wird. Wieder andere Implementierungen wählen kryptografische Hash-Funktionen, für die es (noch) keine ASICs gibt. Wiederholt entstehen Forks und Anpassungen existierender Blockchain-Implementierungen, um neuen technologischen Entwicklungen entgegenzuwirken und die Integrität trotz neuer Technologien aufrechtzuerhalten oder andere neue Technologien zu berücksichtigen sowie auf geänderte Rahmenbedingungen reagieren zu können.

Erweitern der Blockchain durch zusätzliche Abstraktionsschichten

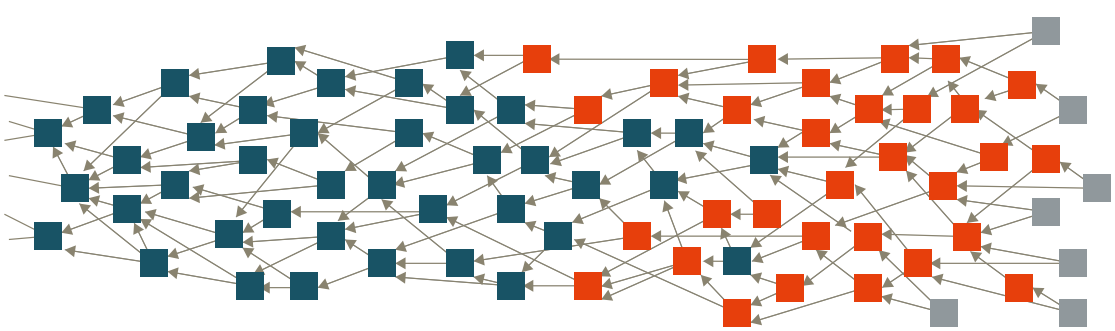
Ende 2017 betrugen die Transaktionsgebühren im Bitcoin-Netzwerk mehr als 50 US-Dollar pro Transaktion und auch heute liegen die Gebühren bei deutlich über einem US-Dollar.[48] Wie viele unbestätigte Transaktionen gerade im Netzwerk auf Bestätigung warten, kann im Blockchain-Explorer der Bitcoin-Blockchain[49] live beobachtet werden, aktuell sind dies mehr als 3.000 Transaktionen – eine Folge aus der Überbelastung des Netzwerks. Zu Beginn des Kapitels wurde gezeigt, dass bei (technischen oder konzeptionellen) Änderungen an der Blockchain verschiedene Abspaltungsvarianten möglich sind. Um das Skalierungsproblem von Bitcoin zu lösen, wurde 2015 in einem Whitepaper von Joseph Poon und Thaddeus Dryja das Lightning-Netzwerk (vgl. Poon/Dryja, 2016)[50] als Skalierungsprotokoll für Blockchains vorgeschlagen. Das Protokoll wird als Abstraktionslayer, also als zusätzliche Schicht oberhalb der Blockchain konzipiert und löst nicht nur das Problem der Skalierbarkeit der Bitcoin-Blockchain, sondern ermöglicht auch minimale Transaktionsgebühren (sogenannte Micro-Payments)[51] und erhöht zudem die Privatsphäre der Teilnehmer. Eine erste Implementierung für das Bitcoin-Netzwerk wurde im März 2018 als Beta-Version freigegeben, wobei die Entwickler konstatieren, dass sich das Netzwerk noch im Pionier- und Teststadium befindet. Ähnlich dem Lightning-Netzwerk sind viele weitere zusätzliche Abstraktionsschichten möglich, um das Basis-Protokoll der jeweiligen Blockchain zu erweitern.

Alternative Datenstrukturen für Distributed-Ledger-Technologien

Auch die Datenstruktur der Blockchain, also die Anordnung von Transaktionen in einer kryptografisch verbundenen Kette von Blöcken, steht auf dem Prüfstand. Der Vollständigkeit halber sollen zwei Distributed-Ledger-Ansätze gezeigt werden, die nicht auf einer Blockchain basieren. Die Kryptowährung IOTA[52] ist konzipiert als Bezahlsystem für das Internet of Things, bei dem keine Transaktionskosten anfallen und somit Mikrotransaktionen (zum Beispiel für die Machine-to-Machine-Kommunikation) möglich sind und zudem das Skalierungsproblem von Blockchains gelöst scheint. Während die bisherigen Darstellungen die Blockchain als einfach verkettete, also lineare Liste beschrieben haben, verwendet IOTA einen gerichteten azyklischen Graphen (DAG). DAGs werden umgangssprachlich als „Tangle“ (vgl. Popov, 2018) bezeichnet.

ABBILDUNG 23: DER TANGLE VON IOTA

Die Anzahl der neu hinzugefügten Transaktionen im IOTA-Tangle ist prinzipiell unbegrenzt, denn jede neue unbestätigte Transaktion (grau) wird durch zwei andere Transaktionen bestätigt. Eine Transaktion ist blau, wenn von jedem Tip ein Pfad zu dieser Transaktion existiert.



Quelle: https://iotasupport.com/cm/images/image02.png. Abgerufen am 29.05.2019.

Jede (bestätigte) Transaktion zeigt im Tangle auf zwei ältere Transaktionen („Eltern"), sodass ein zyklenfreier, gerichteter Graph entsteht. Abbildung 23 stellt rechts in Grau mehrere unbestätigte Transaktionen (sogenannte „Tips") dar, das heißt, Eltern, die keine Kinder haben (Eltern und Kinder sind eine in der Graphentheorie übliche Bezeichnungsweise). Die rotfarbenen Transaktionen wurden bereits validiert und haben mindestens ein Kind. Eine Transaktion ist blau, wenn von jedem Tip ein Pfad zu dieser Transaktion existiert. Die (theoretische) Idee dahinter ist, dass mit der Validierung einer Transaktion auch die Richtigkeit der Eltern überprüft wird und die Korrektheit älterer Generationen ab einem bestimmten Punkt als gegeben angenommen werden kann und dementsprechend nicht mehr geprüft werden muss. Mit der Ausrichtung als Graph und nicht als Kette ist die Anzahl der neu hinzugefügten Transaktionen im IOTA-Tangle prinzipiell unbegrenzt, denn jede neue Transaktion wird durch zwei andere Transaktionen bestätigt, sodass auch immer mehr Transaktionen bestätigt werden, wenn die Zahl der Sender ansteigt. Das bedeutet, dass der IOTA-Tangle proportional mit der Anzahl von Transaktionen skaliert. Interessant ist zudem das Bestreben der Entwickler, den IOTA-Tangle mit speziellen Hash-Funktionen quantensicher zu gestalten. Eine dritte Distributed-Ledger-Technologie stellt der Hashgraph (vgl. Abraham, 2018), entwickelt von Leemon Baird von der Firma Swirlds (vgl. Baird, 2016), dar. Dabei handelt es sich sowohl um eine Datenstruktur als auch um ein Konsensverfahren. Zu den Kerneigenschaften zählen niedriger Energieverbrauch, geringe Speicheranforderungen, höhere Transaktionsgeschwindigkeit von mehr als 250.000 Transaktionen/Sekunde und eine hohe Sicherheit. Allerdings ist Hashgraph nicht Open Source und wurde als Technologie von der Firma Swirlds patentiert.

3.8.4 AUSGESTALTUNG DER BLOCKCHAIN-TECHNOLOGIE FÜR ANWENDUNGEN

Abschnitt 2.6 hat anhand von Beispielen dargestellt, wie zahlreich und vielfältig die Möglichkeiten sind, eine Blockchain (oder einen Distributed Ledger) anzulegen und auszugestalten. Von der grundlegenden Architektur (zentralisiert, quasi-zentralisiert) über den Typus der Blockchain (public/private oder permissionless/permissioned), die eingesetzten Konsensverfahren und die verwendeten Hash-Funktionen bis hin zu Zusatzschichten, um das grundlegende Protokoll zu erweitern, sind viele Stellschrauben vorhanden, um eine quelloffene (Open-Source-) Basisimplementierung an eigene Bedürfnisse anzupassen. Aufgrund der zahlreichen Anwendungsmöglichkeiten, die Distributed Ledgers allgemein (und Blockchain im Speziellen) bieten, kann nur schwer ein „Universalrezept" formuliert werden – zu groß sind die Abhängigkeiten von anwendungsspezifischen Anforderungen.

3.9 Forschungsfragen

Die Untersuchung „Mythos Blockchain: Herausforderung für den öffentlichen Sektor" vom Kompetenzzentrum öffentliche Informationstechnologie (vgl. Welzel et al., 2017) stellt typische Forschungsfragen zusammen, die der Leser nach dem Studium der vorliegenden Studie größtenteils in der Lage ist zu beantworten:

- Welche Alternativen zum energieaufwendigen Prozess des Mining sind möglich bzw. wie kann der Energieaufwand für das Mining reduziert werden? (siehe Abschnitte 2.4, 2.7, 2.8, 2.9, 3.2, 3.8)
- Wie können die Zeiten bis zur Validierung einer Transaktion verkürzt werden? (siehe Abschnitt 3.8)

- Wie können Performanz und Skalierung der Technologie verbessert werden? (siehe Abschnitt 3.8)
- Wie können technologische Anpassungen vorgenommen werden, wenn es keinen zentralen Ansprechpartner gibt? (siehe Abschnitte 2.2, 3.8)
- Wie verträgt sich die Unveränderbarkeit der Blockchain mit dem Recht auf Vergessen? Wie geht man mit irrtümlichen Falschbuchungen um? (siehe Abschnitte 3.2, 3.8)
- Welche weiteren Angriffsmuster sind denkbar und wie kann man sich dagegen absichern? (siehe unter anderem Abschnitt 3.8. Dedizierte Angriffsmuster hängen vor allem von der jeweiligen Blockchain-Implementierung und -Anwendung ab.)
- Wie können Anwendungen von einer Blockchain zu einer anderen migrieren? (siehe Abschnitte 3.6, 3.8)
- Welche Daten sollten in einer Blockchain gespeichert werden und wie sollte dies geschehen? (Diese vermeintliche Forschungsfrage ist in erster Linie eine Design-Frage der jeweiligen Implementierung)
- Wie werden Datenhaltung und Blockchain miteinander verbunden? (siehe Abschnitte 2.4, 2.6)
- Die Absicherung durch rein technische und sehr komplexe Mechanismen, die nur von Experten nachvollzogen werden können, kann den Eindruck erwecken beziehungsweise verstärken, einer Technologie ausgeliefert zu sein. Wie geht man mit den damit entstehenden Ängsten und Vorbehalten um?
- Wie ertüchtigt man Nutzer im Umgang mit der Kryptografie, insbesondere der Absicherung der privaten Schlüssel?

Die beiden letzten Fragen sind sicherlich kein Blockchain-spezifisches Problem, sondern mehr eine gesellschaftliche Frage der Medien- und Technikkompetenz zum verantwortungsbewussten Umgang mit Informationstechnik. Insgesamt ist zu sehen, dass sich Forschungsfragen im Fall der Blockchain nicht zwangsläufig aus der Technologie, sondern vor allem aus der konkreten Anwendung heraus ergeben und eine kritische Reflexion der in Kapitel 3 genannten Merkmale erfolgen muss.

Anhang B stellt ein exemplarisches Werkzeug zur Verfügung, mit dem der Einsatz einer Blockchain für ein vorliegendes Einsatzszenario reflektiert werden kann. Ein Evaluationsfragebogen gibt bei einer einführenden Prüfung zunächst Orientierung, ob eine Blockchain für den jeweiligen Anwendungsfall eine (Problem-)Lösung, auch im Vergleich zu traditionellen Ansätzen, darstellen kann. Bei einer denkbaren Maximalpunktzahl von 16 könnten zum Beispiel mindestens acht mit „Ja“ beantwortete Punkte als Schwellenwert festgelegt werden, ab dem der Einsatz einer Blockchain sinnvoll erscheint und die genauen Anforderungen spezifiziert und mit den verschiedenen technologischen Gestaltungsvarianten und Governance-Optionen in Einklang gebracht werden müssen.

Kapitelendnoten

14 Die Seite www.blockchain.info zeigt zahlreiche Daten und Statistiken rund um die Bitcoin-Blockchain. Unbestätigte (also verifizierungsnotwendige) Transaktionen können auf dieser Seite in Echtzeit beobachtet werden: https://blockchain.info/unconfirmed-transactions.

15 Unter https://bitinfocharts.com/de/top-100-richest-bitcoin-addresses.html sind die finanzstärksten Bitcoin-Adressen aufgelistet. Die Seite https://blockchain.info/popular-addresses zeigt die transaktionsstärksten Adressen an.

16 Forschungsprojekte wie zum Beispiel „BITCRIME" haben es sich zur Aufgabe gemacht, Finanzbetrug zu unterbinden und Benutzer ggf. zu deanonymisieren. Siehe: Verfolgung und Prävention organisierter Finanzkriminalität mit virtuellen Währungen (BITCRIME), https://www.bitcrime.de/index.html, abgerufen am 29.05.2019.

17 Ebd.

18 Ebd.

19 Laut Artikel 4 Nummer 7 der DSGVO ist „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

20 Als „Proof-of-Existence"-Plattformen können exemplarisch genannt werden: Proof of Existence, http://www.proofofexistence.com sowie Origin Timestamp, http://www.originstamp.org.

21 Wie eine solche Dokumentation der Urheberschaft aussehen kann, zeigt der Artikel: Flinterhoff, A. (2018). „Urheberrecht oder Eigentümerschaft mit der Blockchain digital absichern – für Kreative, Kunsteigentümer und Rechteinhaber". Abgerufen am 29.05.2019 von https://www.xing.com/communities/posts/urheberrecht-oder-eigentuemerschaft-mit-der-blockchain-digital-absichern-fuer-kreative-kunsteigentuemer-1014389687.

22 Tatsächlich wird die Kryptowährung nur virtuell empfangen, der Vorgang ist lediglich eine Umbuchung auf der Blockchain.

23 Slock.it (Internetseite). Abgerufen am 29.05.2019 von https://slock.it.

24 Eine Liste der Mitglieder im Projekt Hyperledger ist zu finden unter: https://www.hyperledger.org/members, abgerufen am 29.05.2019.

25 Übersicht zu IBMs Hyperledger Fabric, https://www.ibm.com/blockchain/de-de/hyperledger.html, abgerufen am 29.05.2019.

26 Weitere Informationen zum Projekt Hyperledger Burrow unter: https://www.hyperledger.org/projects/hyperledger-burrow, abgerufen am 29.05.2019.

27 Weitere Informationen zum Projekt Hyperledger Iroha unter: https://www.hyperledger.org/projects/iroha, abgerufen am 29.05.2019.

28 Weitere Informationen zum Projekt Hyperledger Indy unter: https://www.hyperledger.org/projects/hyperledger-indy, abgerufen am 29.05.2019.

29 Weitere Informationen zum Projekt Hyperledger Sawtooth unter: https://www.hyperledger.org/projects/sawtooth, abgerufen am 29.05.2019.

30 Weitere Informationen zur Seafood Case Study in: Supply Chain Traceability Using Blockchain Technology unter: https://www.hyperledger.org/projects/sawtooth/seafood-case-study, abgerufen am 29.05.2019.

31 Dies entspricht ca. 50.000 Transaktionen pro Sekunden, https://ripple.com/xrp/, abgerufen am 29.05.2019.

32 Cryptolist (Internetseite). Die Kryptowährung Zcash (ZEC). Abgerufen am 29.05.2019 von https://www.cryptolist.de/zcash.

33 CoinMarketCap (Internetseite). All Cryptocurrencies. Abgerufen am 29.05.2019 von https://coinmarketcap.com/all/views/all/.

34 Mehr Informationen zur Social-Media-Plattform Steemit unter: https://steemit.com.

35 Mehr Informationen zum Projekt Enerchain: Abgerufen am 29.05.2019 von https://enerchain.ponton.de.

36 Mehr Informationen zum Unternehmen Cryptofuture: Abgerufen am 29.05.2019 von https://www.cryptofuture.com.

37 Mehr Informationen zur Open-Innovation-Plattform der Initiative Intelligente Vernetzung: Abgerufen am 29.05.2019 von https://www.oip.netze-neu-nutzen.de/home/.

38 Weitere Informationen zu Whats2doo unter: https://www.whats2doo.com/, abgerufen am 29.05.2019.

39 Weitere Informationen zur Applikation fizzy der AXA unter: https://fizzy.axa/en-gb/, abgerufen am 29.05.2019.

40 Weitere Informationen zu Estlands digitalen Verwaltungsdiensten unter: Building blocks of e-estonia, https://e-estonia.com/solutions/, abgerufen am 29.05.2019.

41 Weitere Informationen zum Projekt ResearchProof unter: An online digital logbook to protect and prove authorship, and to share scientific results, https://www.fabiodisconzi.com/open-h2020/projects/211312/index.html, abgerufen am 29.05.2019.

42 Weitere Informationen zum R3-Konsortium unter: R3 – The distributed database technology company, https://www.r3.com/, abgerufen am 29.05.2019.

43 Weitere Informationen zum offenen Standard unter: Blockcerts: The Open Standard for Blockchain Credentials, https://www.blockcerts.org, abgerufen am 29.05.2019.

44 Nähere Informationen hierzu unter: Burst Explorer, https://explore.burst.cryptoguru.org/chart/supply/network_size, abgerufen am 29.05.2019.

45 Weitere Informationen zu Decred unter: https://docs.decred.org/, abgerufen am 29.05.2019.

46 Weitere Informationen zu VeChain unter: https://www.vechain.com/#/support/01, abgerufen am 29.05.2019.

47 Weitere Informationen zur Nem-Blockchain unter: https://nem.io, abgerufen am 29.05.2019.

48 Bitcoin Avg. Transaction Fee historical chart, https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#1y, abgerufen am 29.05.2019.

49 Die noch unbestätigten Transaktionen auf der Bitcoin-Blockchain können hier eingesehen werden: https://blockchain.info/unconfirmed-transactions/, abgerufen am 29.05.2019.

50 Poon, J., Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Abgerufen am 29.05.2019 von https://lightning.network/lightning-network-paper.pdf.

51 Anmerkung: Durch effiziente Micro-Payments kann der „träge Bitcoin“ für IoT-Anwendungen wieder interessant werden.

52 Weitere Informationen zu IOTA unter: What is IOTA, https://iotasupport.com/whatisiota_de.shtml, abgerufen am 29.05.2019.

04

EINSATZ DER BLOCKCHAIN-TECHNOLOGIE IM HOCH-SCHULBILDUNGSSYSTEM

Dieses Kapitel beleuchtet das theoretische Potenzial der Anwendung von Blockchain-Technologie auf dem Feld der Hochschulbildung. Es betrachtet zunächst die technischen und ökonomischen Grundlagen der Blockchain, um derart informiert die Blockchain-Technologie und ihre verschiedenen Ausprägungen in den gesellschaftlichen Kontext zu stellen und in verschiedenen Anwendungsgebieten kritisch zu diskutieren. Aufbauend auf der EU-Studie „Blockchain in Education" (Grech/Camilleri, 2017) werden Einsatzszenarien von Blockchain im Hochschulbildungsbereich entwickelt. Im Mittelpunkt stehen insbesondere solche Szenarien, die kurz- bis mittelfristig einen hohen Impact für die Weiterentwicklung von hochschulübergreifenden Strukturen erwarten lassen. Alle aufgeführten Szenarien sind dabei prinzipiell sowohl auf das grundständige Studium wie auf die wissenschaftliche Weiterbildung anwendbar. Die Szenarien werden im soziotechnischen Kontext diskutiert (einführend hierzu siehe Abschnitt 4.1) und entlang der im Kapitel 3 insbesondere in den Abschnitten 3.1 bis 3.4 sowie 3.7 entwickelten Eigenschaften und getroffenen Unterscheidungen eingeordnet. Abschnitt 4.9 fasst schließlich die Einschätzungen von Stakeholdern im deutschen Hochschulbildungssystem sowie von internationalen Experten für „Blockchain in Education" zu den entwickelten Szenarien sowie zur weiteren Entwicklung des Felds zusammen.

4.1 Spezifische Rahmenbedingungen für den Einsatz der Blockchain-Technologie im deutschen Hochschulbildungssystem

Zur Analyse der Gegebenheiten in Deutschland im Hinblick auf geeignete Anwendungsmöglichkeiten der Blockchain-Technologie werden insbesondere die folgenden für Deutschland spezifischen Merkmale berücksichtigt:

↖ RAHMENBEDINGUNGEN DES DEUTSCHEN HOCHSCHULSYSTEMS

Hohes Maß an Subsidiarität und Autonomie

Das deutsche Hochschulbildungssystem ist durch die Gesetzgebung der einzelnen Länder geregelt. Außerdem verfügt jede Hochschule bei der Festlegung ihrer eigenen Verfahren und Systeme über ein hohes Maß an Autonomie. Dennoch muss die Anerkennung von Bildungsnachweisen aller Art in ganz Deutschland (und in Europa) gewährleistet sein. Da das deutsche Hochschulbildungssystem somit aus zahlreichen miteinander interagierenden Subsystemen besteht, verlangt diese Situation aus systemarchitektonischer Sicht nicht nach Zentralisierung, sondern nach dezentral geführten und gleichwohl interoperablen Systemen.

Öffentlich getragene Hochschulbildung

Hochschulbildung wird in Deutschland überwiegend durch staatlich getragene und finanzierte Institutionen vermittelt – ein Modell, das in Politik und Öffentlichkeit ein hohes Maß an Unterstützung genießt. Einsatzszenarien der Blockchain-Technologie sollten daher darauf ausgerichtet sein, die staatlichen Ziele für die Hochschulbildung zu stärken und zu unterstützen.

Mangelndes Vertrauen in zentrale Datensammlung

Deutschland gehört weltweit zu den Staaten mit den schärfsten Datenschutzbestimmungen, den wirksamsten Instrumenten zur Durchsetzung des Datenschutzes und der höchsten öffentlichen Unterstützung für solche Regelungen. Gesellschaftlich ist Deutschland bestrebt, keinem Akteur, einschließlich der Regierung, zu viel Kontrolle über und Zugang zu sensiblen persönlichen Daten zu gewähren. Jedes vorgeschlagene System sollte daher darauf ausgerichtet sein, mit einem solchen Ziel in Einklang zu stehen bzw. ein solches Ziel zu stärken.

Begrenzte Innovation in Campusmanagementsoftware

Die Marktkonzentration im Bereich der Hochschulinformations- und Campusmanagementsoftware auf wenige Anbieter lässt zunächst wenig Innovationskraft und einen übergroßen Fokus auf die internen Anforderungen der Hochschulen vermuten. Ein Hinweis darauf mag sein, dass im Jahr 2018 insbesondere die Abschlüsse der Studierenden nach wie vor hauptsächlich in Papierform ausgestellt, archiviert, weitergegeben und verifiziert werden – trotz bereits weitgehend elektronisch erfolgender Prüfungsverwaltung. Dies führt auch außerhalb des Hochschulbereichs zu hochgradig ineffizienten Verfahren, etwa bei Arbeitgebern, die diese Bildungsnachweise verifizieren möchten. Jede Verbesserung des Systems sollte daher Effizienzsteigerungen für alle Akteure im Bildungsbereich im Blick haben.

Die vorgestellten Merkmale fließen in die Bewertung der verschiedenen Szenarien zum Einsatz der Blockchain-Technologie im Hochschulbildungssystem ein. Im Folgenden werden fünf Bereiche mit hohem Potenzial für Blockchain-Technologie im Bildungsbereich umrissen.

4.2 Szenarien des Einsatzes und Anwendungsfälle von Blockchain im Hochschulbildungsbereich

Da die Blockchain-Technologie unter Berücksichtigung der in Kapitel 2 dargestellten Regeln geeignet ist, jede auf Bestandsbüchern (ledgers) basierende Datenbank zu ersetzen, wird in den folgenden Szenarien nicht nur berücksichtigt, was technisch möglich ist, sondern insbesondere auch, ob die Anwendung der Blockchain-Technologie

für das Szenario einen signifikanten Vorteil für den Anwendungsfall bietet und ob es bereits Start-up-Aktivitäten auf diesem Gebiet gibt, die in absehbarer Zeit eine Anwendung im Hochschulbildungsbereich möglich erscheinen lassen.

Ausgehend von den in der EU-Studie beschriebenen Szenarien und der Ausgangslage im deutschen Hochschulbildungssystem weisen insbesondere die folgenden fünf Bereiche vielversprechende Potenziale für den Einsatz und Anwendungsfälle von Blockchain im Hochschulbildungsbereich auf (siehe auch das Verzeichnis auf S. 10):

» Bildungsnachweise beglaubigen, ausstellen und anerkennen (Abschnitt 4.3)
» Software und Daten in Lehre und Studium dezentralisieren (Abschnitt 4.4)
» Studierendendaten in der Verwaltung minimieren (Abschnitt 4.5)
» Akademische Inhalte und Werke nachverfolgen (Abschnitt 4.6)
» Zahlungen und Mittelflüsse managen (Abschnitt 4.7)
» Weitere Szenarien (Abschnitt 4.8)

Die Auswahl dieser Szenarien wurde im Rahmen der Diskussionen mit Stakeholdern und Experten validiert (siehe Abschnitt 4.9). In den folgenden Abschnitten wird jedes dieser Szenarien detailliert beschrieben.

Innerhalb der Szenarien werden in diesem Bericht auch Anwendungsfälle diskutiert, mit denen die Szenarien jeweils beschrieben werden können. An Anwendungsfälle wiederum lassen sich spezifische Empfehlungen für den Einsatz im deutschen Hochschulbildungssystem anknüpfen (siehe Abbildung 24).

SZENARIEN, ANWENDUNGSFÄLLE UND IMPLEMENTIERUNGEN

ABBILDUNG 24: UNTERSCHEIDUNG UND BEZIEHUNG VON SZENARIO, ANWENDUNGSFALL UND IMPLEMENTIERUNG VON BLOCKCHAIN-TECHNOLOGIE

Quelle: Eigene Darstellung

Die analytische Struktur zur Diskussion jedes Szenarios beinhaltet folgende Aspekte:

» *Hintergrund:* Beschreibung des Systems, das heißt, der Gesamtaktivitäten, die innerhalb des Kontexts und des Anwendungsbereichs des Szenarios stattfinden.
» Ausgangslage: eine Diskussion der spezifischen Probleme, die sich aus dem Status quo ergeben, sei es aus der Struktur und/oder aus der Governance der zugrundeliegenden Ledger-Technologien, die derzeit zur Anwendung kommen.
» *Beschreibung des Einsatzes von Blockchain:* detaillierte Darstellung der Art und Weise, wie Blockchain-Technologien eingesetzt werden könnten, um den Status quo zu verbessern und die beschriebenen Limitierungen zentralisierter Ledger-Systeme zu überwinden.
» *Potenziale des Einsatzes von Blockchain:* beschreibt, wie Blockchain die beschriebenen Herausforderungen adressieren kann, und betont den allgemeinen Nutzen, den eine Anwendung des Szenarios für die Akteure mit sich zu bringen verspricht.

- *Anwendungsfälle:* spezifische Beispiele für Dienste, die mithilfe von Blockchain eingeführt werden könnten.
- *Analyse:* beschäftigt sich mit Problemen, die die Umsetzbarkeit solcher Szenarien beeinträchtigen und in den Szenarien selbst begründet liegen, darunter:
  - *Marktreife:* beschreibt, inwiefern die aktuelle Technologie bereit für die Anwendung des Szenarios ist. Da es sich bei Blockchain um eine ganz neue Technologie handelt, existieren keine Beispiele für flächendeckende Anwendungen im Bildungsbereich. Deshalb werden stellvertretend existierende Projekte, Blockchain-Start-ups und Pilotimplementierungen in früheren Entwicklungsphasen untersucht.
  - *Kosten- und Zeitersparnisse:* untersucht die Gesamteffizienz und -wirksamkeit der Implementierung von Blockchain-Technologie in dem Szenario als zentralen Faktor bei der Entscheidung zur Berücksichtigung von Blockchain.
  - *Voraussetzungen:* identifiziert technologische oder regulatorische Entwicklungen, die für die Realisierbarkeit der Szenarien eintreten müssten.
  - *Perspektiven:* nimmt ausgehend von den oben genannten Faktoren eine Einschätzung der Wahrscheinlichkeit und des Zeitrahmens einer Umsetzung vor.

Die Darstellung der einzelnen Szenarien erfolgt weitestgehend wertneutral, da die Einschätzung und Attraktivität einer Implementierung von Blockchain in jedem Szenario von zahlreichen Faktoren abhängt, die die Art und Weise der Umsetzung und insbesondere die technische und Governance-Architektur des Systems bestimmen. Auf Basis dieser Darstellung lassen sich zu jedem Szenario bzw. Anwendungsfall individuelle SWOT-Analysen erstellen, die in hohem Maße davon abhängen, welcher Stellenwert jeweils den technischen Eigenschaften und soziotechnischen Mehrwerten der Blockchain wie Dezentralisierung, Selbstbestimmung, Unveränderbarkeit, Transparenz und freiem Zugang (siehe Abschnitte 3.1, 3.3) beigemessen wird.

4.3 Bildungsnachweise beglaubigen, ausstellen und anerkennen

4.3.1 HINTERGRUND

Der folgende Abschnitt behandelt die Beglaubigung, Ausstellung und Anerkennung von Bildungsnachweisen. Der JRC-Bericht „Blockchain in Education“ (Grech/Camilleri, 2017) definiert Zertifizierung im Kern als schriftliche Aussage einer Partei gegenüber einer anderen Partei, dass bestimmte Fakten der Wahrheit entsprechen. Jede Form der Zertifizierung enthält somit die folgenden Komponenten:

↖ **KOMPONENTEN EINES ZERTIFIKATS**

- *Claim:* die Aussage, dass „diese Fakten der Wahrheit entsprechen“. Beispiele im Bildungskontext wären Aussagen wie „ein Lernender hat eine Kompetenz erworben“, „eine Lehrkraft verfügt über ausreichend Wissen für den Unterricht“ oder „eine Studentin hat eine Aufgabe erfolgreich beendet“.
- *Aussteller:* eine Instanz, die nach Überprüfung und Validierung der Fakten bestätigt, dass der Claim wahr ist.
- *Belege:* zur Unterstützung des Claims, üblicherweise unter Einbezug der Verfahren, mit denen die Behauptung verifiziert wird, sowie einigen Zusatzinformationen zum Claim. Zertifiziert eine Hochschule beispielsweise, dass eine Studierende einen ECTS-Punkt für ihre Leistung erhalten hat, so sind im ECTS-Handbuch die Komponenten und Verfahren zur Verifizierung dieses Claims dargelegt. Bei diesem Beispiel besteht das Verfahren darin, die Studierende im Hinblick auf das Erreichen

spezifischer Lernergebnisse zu prüfen, die durch einen Lernaufwand von ungefähr 25 Stunden erreicht wurden.
- *Empfänger:* die Person, über die der Claim aufgestellt wird: der Lernende, der eine Kompetenz erwirbt; die Lehrkraft, die über ausreichend Wissen für den Unterricht verfügt; oder die Studierende, die eine Aufgabe erfolgreich beendet hat.
- *Zertifikat:* ein Dokument, das die Identität des Ausstellers, die Identität des Empfängers sowie den Claim bestätigt und auf die erforderlichen Belege verweist.
- Jedes Zertifikat enthält eine Signatur, die ausschließlich vom Aussteller angebracht werden kann und somit dessen Identität bestätigt: ein besonderes Symbol, ein Stempel, ein Bild oder ein Code.

ZERTIFIZIERUNGSPROZESS

Die Zertifizierung besteht aus drei klar voneinander abgegrenzten Prozessen:

- *Ausstellung:* der Prozess, mit dem Claim, Aussteller, Belege, Empfänger und Signatur auf einem Zertifikat festgehalten werden. Häufig werden die Daten in einer zentralisierten Claim-Datenbank und/oder auf einem Zertifikat festgehalten, das dem Nutzer ausgehändigt wird.
- *Verifizierung:* der Prozess, mit dem Dritte die Echtheit des Zertifikats überprüfen. Dies kann auf drei Wegen geschehen:
  1. Verifizierung mithilfe von im Zertifikat integrierten Sicherheitsmerkmalen wie Siegel, Sicherheitspapier oder Signaturen
  2. Verifizierung durch Kontaktaufnahme mit dem Aussteller des Zertifikats. In diesem Fall stellt die dritte Partei eine Anfrage an die ausstellende Instanz, ob das Zertifikat tatsächlich dort ausgestellt wurde. (Der Aussteller könnte dann eine Abfrage in seiner zentralisierten Claim-Datenbank durchführen oder die Echtheit anhand von Sicherheitsmerkmalen im Zertifikat überprüfen.)
  3. Verifizierung durch Abgleich mit einer zentralisierten Claim-Datenbank. In diesem Fall hat der Aussteller alle ausgestellten Zertifikate in eine Drittdatenbank eingestellt, auf die jeder zugreifen kann, um Kopien aller ausgestellten Zertifikate einzusehen und zu vergleichen.
- *Weitergabe:* der Prozess, mit dem der Empfänger eines Zertifikats dieses an Dritte weiterleitet. Die Weitergabe kann auf drei Wegen erfolgen:
  1. Direkte Weitergabe des Zertifikats (oder einer Kopie) an Dritte, zum Beispiel per E-Mail oder durch persönliche Vorlage.
  2. Hinterlegung des Zertifikats bei einer Stelle, die nur bestimmten, vom Empfänger autorisierten Personen Zugriff darauf gewähren darf. (Beispiel: Bei einem privaten Testament darf der Notar nach dem Tod des Erblassers den Inhalt nur den Nutznießern mitteilen.)
  3. Veröffentlichung des Zertifikats durch Ablage in einem öffentlichen Register oder Archiv, wo es offen einsehbar ist.

ZERTIFIKATE UND IHRE SPEZIFISCHEN ZWECKE

Zertifikate sind im Bildungsbereich weit verbreitet und werden für unterschiedliche Zwecke verwendet. Mit der Ausstellung eines Zertifikats wird den Lernenden üblicherweise Folgendes bescheinigt:

- *Abschluss eines spezifischen Bildungsgangs.* Beispiel: Schulabgangszeugnis im formalen Bildungssektor oder Zertifikat zur Bescheinigung der Teilnahme an einem Austauschprogramm.
- *Gesamtheit des Erlernten auf einem bestimmten Fachgebiet.* Beispiel: Zertifikat über die Verleihung eines Hochschulabschlusses.
- *Abschluss einzelner Lerneinheiten durch das Erreichen spezifischer Lernziele.* Beispiel: ECTS-Credits im Hochschulbildungssystem.
- *Spezifische Vorerfahrungen.* Beispiel: Zertifikate über den Abschluss einer Berufsausbildung oder einer anderen Form von Arbeitserfahrung.

- *Erwerb von spezifischen Fertigkeiten.* Beispiel: Zertifikate im Rahmen der Anerkennung von Vorkenntnissen.
- *Erreichen von bestimmten Exzellenzkriterien.* Beispiel: Gewinn von Preisen für besondere Leistungen oder Universitätsabschluss „summa cum laude".
- *Erreichen eines bestimmten Kompetenzniveaus in spezifischen Fachgebieten* durch die Ausstellung von Prüfungszertifikaten oder Zeugnissen.

Zwar werden die meisten Bildungsnachweise im Hochschulbereich nach wie vor in Papierform ausgestellt, doch einige Institutionen haben mit der Ausstellung von digitalen Bildungsnachweisen auf Grundlage von Public-Key-Infrastrukturen (siehe Abschnitt 2.5) begonnen. Seit Dezember 2017 versieht beispielsweise die Universität Göttingen ihre Bachelor- und Masterzeugnisse und -urkunden mit einer digitalen Signatur.[53] Aufgrund der nachfolgend beschriebenen Einschränkungen bleibt die Digitalisierung von Bildungsnachweisen jedoch weiterhin eher die Ausnahme als die Regel.

4.3.2 AUSGANGSLAGE

Der folgende Abschnitt führt die wesentlichen Einschränkungen von Zertifizierungsprozessen an Bildungseinrichtungen aus und geht hierbei auf technische und organisatorische Einschränkungen sowie den Aspekt des eingeschränkten Vertrauens ein.

Technische Einschränkungen

Mit allen Bildungsnachweisen gibt es ähnliche Probleme, nämlich:

- Die Ausstellung, Verwaltung und Verifizierung dieser Zertifikate ist zeit- und kostenintensiv.
- Public-Key-Infrastrukturen erfordern für die Ausstellung und Verifizierung von Zertifikaten den Einsatz einer Zertifizierungsstelle als Mittlerorganisation. Dadurch entsteht eine Abhängigkeit, die Missbrauch hervorrufen kann. Zertifizierungsstellen haben ihre Stellung traditionell insbesondere dafür genutzt, extrem hohe Gebühren für den Zugang zu ihren Dienstleistungen zu verlangen.
- Originale und Verifizierungsdokumente unterliegen außerdem der Gefahr, durch Misswirtschaft, Naturkatastrophen oder Kriege zerstört zu werden.
- Es gibt einen Mangel an Interoperabilität zwischen verschiedenen Zertifikatstypen.
- Aus Datenschutzsicht erfordert die Verifizierung von Dokumenten entweder,
  - dass die ausstellende Organisation Kopien der Zertifikate vorhält, um die Authentizität von ihr ausgegebener Zertifikate verifizieren zu können, oder
  - dass man sich für die Root-Zertifikate auf eine zentrale Instanz verlässt, oder
  - dass Papierzertifikate mit hinreichend komplexen integrierten Sicherheits- und Fälschungsschutzmerkmalen ausgestellt werden, sodass sie auch ohne Bezugnahme auf eine externe Datenbank als authentisch eingestuft werden können.

Organisatorische Einschränkungen

Aus organisatorischer Sicht weisen Zertifikate die folgenden Einschränkungen auf:

- mangelnde Kompatibilität der technischen Standards für Ausstellung und Zertifizierung,
- uneinheitliche Umsetzung der Regeln, etwa bei der Anerkennung von Auslandsaufenthalten,
- mangelndes Vertrauen, einer einzelnen Organisation die Hauptschiedsfunktion für die Einhaltung der Regeln zu übertragen,
- manuelle Verfahren zur Anerkennung und Verifizierung.

In den vergangenen Jahren hat es insbesondere im Rahmen des Bologna-Prozesses Anstrengungen gegeben, diese Zertifikate zu standardisieren. Doch bis heute gibt es keinen Meta-Standard zur digitalen Beschreibung von ECTS, keine Standard-Datenbank zur Archivierung von ECTS-Punkten und keinen standardisierten Weg zur automatischen Speicherung von ECTS-Punkten. Die Europäische Kommission hat eine Machbarkeitsstudie zur Digitalisierung des Diploma Supplements in Auftrag gegeben und einige EU-geförderte Projekte untersuchen die Machbarkeit eines IKT-gestützten Transfers von Credits. Die von Mozilla initiierte Open-Badges-Initiative versucht, einen Standard für die Zertifizierung non-formaler Bildung zu entwickeln – bislang mit mäßigem Erfolg.

DIE OPEN BADGES INITIATIVE (OBI)

Die Open Badges Initiative (OBI) unterstützt eine Vielzahl an Ausstellern, die digitale Abzeichen (badges) vergeben, sowie eine Vielzahl an Personen, die solche Auszeichnungen erhalten und veröffentlichen, um damit auf ihre Kompetenzen und Leistungen aufmerksam zu machen. Jeder Nutzer kann von vielen verschiedenen Ausstellern Auszeichnungen erhalten und diese an einem mit der eigenen Identität verknüpften Ort sammeln, um sie dann mit verschiedenen Webseiten und Zielgruppen zu teilen (zum Beispiel Karriereportalen, sozialen Netzwerken oder persönlichen Portfolios). OBI will die Ausstellung, Sammlung und Veröffentlichung von Badges fördern. Dazu gehört, Inhabern von Badges die Möglichkeit zu geben, die Badges mit ihrer Internet-Identität zu verknüpfen und sie überallhin mitzunehmen, sowie den Inhabern der Badges zu ermöglichen, die Badges Dritten zu zeigen (zum Beispiel Arbeitgebern, Hochschulverwaltungen, Kollegen). Inhabern von Badges soll es möglich sein, ihre Sammlungen zu verwalten und die Sichtbarkeit dieser Sammlungen zu kontrollieren. Die gesamte Initiative und Infrastruktur ist offen und dezentralisiert, um den website- und ausstellerübergreifenden Transfer von Badges zu erleichtern.

Das Groningen Declaration Network[54] versucht ebenfalls, diese Einschränkungen zu überwinden, indem im Rahmen eines Stakeholder-Netzwerks zur Portabilität digitaler studentischer Daten darüber diskutiert wird.

Eingeschränktes Vertrauen

In Deutschland und den meisten anderen Ländern ist der Bildungssektor stark reguliert, um sicherzustellen, dass nur qualitativ hochwertige Bildungsangebote verfügbar sind und somit auch die Qualität von Bildungsnachweisen gewährleistet ist. Organisationen, die außerhalb des staatlich regulierten Systems operieren und Bildungsnachweise von geringerer oder zweifelhafter Qualität anbieten, werden gelegentlich als Titelmühlen (englisch diploma mills) bezeichnet. Gegenwärtig existiert kein Zertifikatssystem, mit dem es möglich wäre, automatisch zu überprüfen, ob die ausstellende Organisation ein akkreditierter beziehungsweise zertifizierter Anbieter ist oder nicht beziehungsweise ob Bildungsangebote bestimmte Qualitätsstandards erfüllen oder nicht.

4.3.3 BESCHREIBUNG VON METHODEN ZUR ANWENDUNG VON BLOCKCHAIN-TECHNOLOGIE

Es gibt drei verschiedene technische Methoden, mit denen die Blockchain-Technologie für die Ausstellung und Anerkennung von Bildungsnachweisen genutzt werden könnte:

Methode 1: Blockchain-basierte PKI-Infrastruktur

Auf der Blockchain werden die PKI-Zertifikate gespeichert, die von den Hochschulen zur digitalen Signatur von Dokumenten verwendet werden. Die Bildungsnachweise selbst werden nicht auf der Blockchain abgelegt. Dies würde bedeuten:

» Die Nachweise können vernichtet werden (sind also DSGVO-kompatibel). Eine Bearbeitung ist jedoch nicht möglich.
» Nur Daten über juristische Personen werden auf der Blockchain gespeichert, das heißt, die Daten liegen außerhalb des Geltungsbereichs der DSGVO.
» Eine automatische Verifizierung ist nur für die Identität des Ausstellers möglich – um die Identität des Empfängers zu verifizieren, wäre ein separates (aber möglicherweise integriertes) System notwendig.

Methode 2: Per Blockchain gesicherte digitale Bildungsnachweise

Auf der Blockchain wird ein Hash-Wert des digitalen Bildungsnachweises gespeichert, zusammen mit dem Public Key der ausstellenden Institution und dem Public Key des Empfängers. Der Bildungsnachweis selbst wird nicht auf der Blockchain gespeichert.

Dies würde bedeuten:

» Die Blockchain enthält persönliche Daten gemäß DSGVO.
» Einträge können nicht verändert werden.
» Die automatische Verifizierung der Identität des Empfängers ist möglich.

Methode 3: Auf der Blockchain ausgestellte Bildungsnachweise

Der Inhalt des Nachweises wird auf der Blockchain gespeichert, zusammen mit dem Public Key der ausstellenden Institution und dem des Zertifikatsempfängers. Dies würde bedeuten:

» Die Blockchain enthält persönliche Daten gemäß DSGVO.
» Einträge können nicht verändert werden.
» Eine automatische Anerkennung und Anrechnung von Credits zwischen Institutionen ist möglich, ebenso die automatische Kombination von Qualifikationen *(stackable credentials)*.
» Es kann verhindert werden, dass Qualifikationen kopiert und erneut verwendet werden *(double-spending)*.

4.3.4 POTENZIALE DES EINSATZES VON BLOCKCHAIN

Dieser Abschnitt befasst sich mit der Weiterentwicklung des Status quo von Zertifizierungsprozessen an deutschen Bildungseinrichtungen unter Anwendung der im vorherigen Abschnitt präsentierten Methoden zur Anwendung von Blockchain-Technologien für die Ausstellung und Anerkennung von Bildungsnachweisen.

Bei den ersten beiden Methoden werden die zur Verifizierung der Bildungsnachweise nötigen Belege vollständig, sicher und dauerhaft auf einer Blockchain gespeichert. Somit könnten die von den Nutzern gehaltenen Bildungsnachweise selbst im Falle, dass die ausstellenden Institutionen den Betrieb einstellen oder die Daten

↖ **DIE UNVERÄNDERLICHKEIT VON ZERTIFIKATEN**

durch eine Naturkatastrophe vernichtet werden, durch den Abgleich mit den auf der Blockchain gespeicherten Daten verifiziert werden.

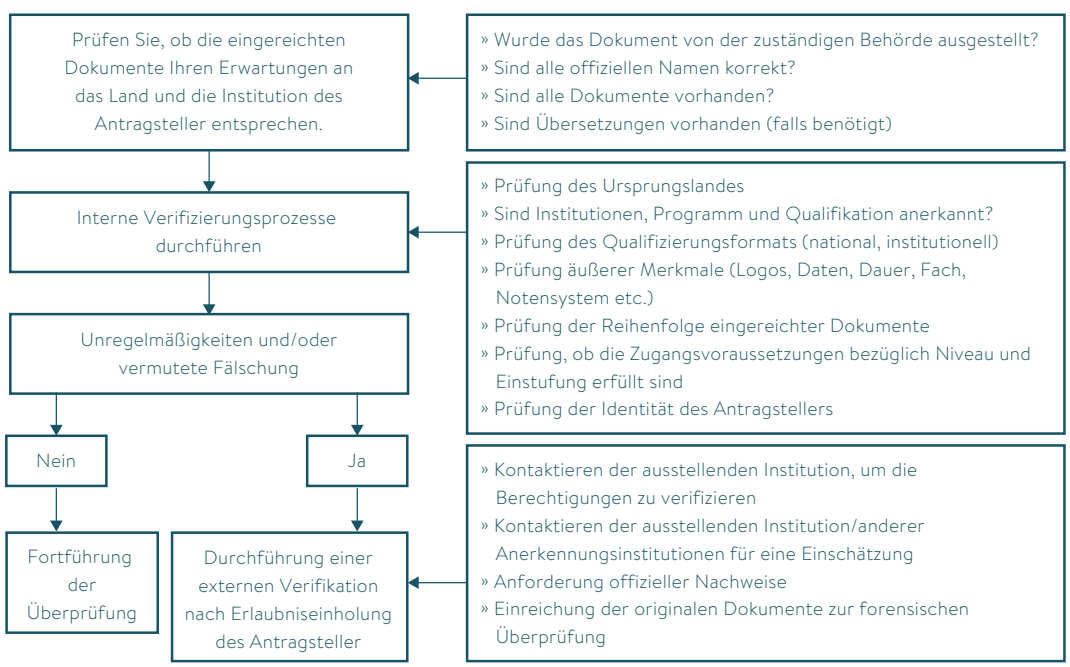
Außerdem müssten die Hochschulen nach der Ausstellung eines Zertifikats keine weiteren Ressourcen mehr aufbringen, um das Zertifikat zu archivieren oder seine Gültigkeit gegenüber Dritten zu bestätigen, denn Letztere könnten die Echtheit der Zertifikate durch einen Abgleich mit den auf der Blockchain gespeicherten Daten jederzeit selbst überprüfen.

Der Hauptvorteil der dritten Methode besteht darin, dass nicht nur die Nachweise der Validität eines Zertifikats auf der Blockchain gespeichert würden, sondern auch das Zertifikat selbst. Damit würden der Authentizitätsnachweis und auch das Zertifikat selbst dauerhaft und unveränderbar.

AUTOMATISCHE ANERKENNUNG UND TRANSFER OF CREDIT

Würden Zertifikate direkt auf einer Blockchain abgelegt, könnten mithilfe von Smart Contracts verschiedene Merkmale zur Übertragbarkeit, Anerkennung beziehungsweise Anrechnung und Kombinierbarkeit von Qualifikationen direkt auf die Blockchain programmiert werden. Dadurch würden der Transfer von Studiennachweisen zwischen Hochschulen, das Verleihen von Abschlüssen und andere Transaktionen, bei denen die Anerkennung bzw. Anrechnung und Ansammlung von Studiennachweisen eine Rolle spielen, automatisch verifiziert und ausgeführt werden. Gegenwärtig muss jede dieser Transaktionen manuell überprüft und von einem Hochschulmitarbeiter genehmigt werden.

ABBILDUNG 25: ENIC-NARIC-ABLAUFPLAN FÜR DIE VERIFIZIERUNG VON BILDUNGSNACHWEISEN



Quelle und nähere Informationen: http://ear.enic-naric.net/emanual/Chapter4/default.aspx, abgerufen am 29.05.2019

Bei allen drei Methoden würden in sogenannten Wallets organisierte Zertifikate bei der Weitergabe als eigenständige Nachweise der Bildungsnachweise fungieren, die sie repräsentieren.

↖ AUTOMATISCHER (SELBST-)NACHWEIS

Insgesamt bietet dieses Szenario den Nutzern granulare Kontrolle über ihre Zertifikate: Die Nutzer könnten bestimmen, wer unter welchen Umständen ein Zertifikat einsehen kann. Ferner würde jede Einrichtung, die Zertifikate verifiziert (zum Beispiel Arbeitgeber oder andere Hochschulen), bei dieser Tätigkeit erhebliche Ressourcen einsparen, weil alles automatisch erfolgen würde.

Die Abbildung 25 zeigt ein Ablaufdiagramm, das für das ENIC-NARIC-Netzwerk zur Verifizierung von Bildungsnachweisen in Europa empfohlen wird. Das Versprechen der Blockchain besteht darin, dass der gesamte Prozess in einem einzigen Klick automatisiert wird.

4.3.5 AUSSTELLUNG BEGLAUBIGTER BILDUNGSNACHWEISE

Als Anwendungsfall könnten Bildungseinrichtungen ihren Schülern und Studierenden als Nachweis erreichter Lernziele digitale Zertifikate ausstellen, die über eine Blockchain beglaubigt sind.

4.3.6 VERIFIZIERUNG VON ZERTIFIKATEN

In einer Welt, in der die Beglaubigung von Zertifikaten auf der Blockchain die Norm darstellt, könnten Einrichtungen eine Software entwickeln, die bei allen internen Prozessen, für die Bildungsnachweise eingereicht werden müssen (zum Beispiel Zulassung zum Studium, Personalgewinnung, Beförderungen), eine automatische Verifizierung der Zertifikate vornimmt. Mithilfe solcher Systeme würden Zertifikate nur dann zur weiteren Bearbeitung an die entsprechende Abteilung weitergeleitet, wenn sie im Rahmen der automatischen Prüfung als echt markiert werden.

4.3.7 VERIFIZIERTE DIGITALE IDENTITÄTEN FÜR HOCHSCHULEN

Die Akkreditierung von Hochschulen und Studiengängen ist ein komplexer Prozess, bei dem jedes Land eigenen, zumeist mehrstufigen Verfahren folgt. Nimmt man Online-Angebote und internationale Qualifikationen hinzu, so gibt es allein in Europa buchstäblich Hunderte verschiedener Akkreditierungsverfahren.

↖ AKKREDITIERUNGSVERFAHREN AUF DER BLOCKCHAIN

Für Nicht-Experten wie Schüler und Studierende kann es somit äußerst schwierig sein, zu erkennen, ob es sich bei einer ihnen unbekannten Institution – besonders im Onlinebereich oder im internationalen Kontext – tatsächlich um eine Einrichtung von anerkannter Qualität handelt. Einige Titelmühlen sind dafür bekannt, dass sie gefälschte Akkreditierungsagenturen und Universitätsnetzwerke gründen, um seriös auszusehen.[55]

Der einzige Weg, um sicher zu wissen, ob eine Einrichtung tatsächlich real ist – insbesondere im Onlinebereich – besteht darin, jede Stufe eines Akkreditierungsverfahrens im Abgleich mit einer Datenbank von „autorisierten“ Abläufen für akkreditierte Institutionen zu verifizieren.

Blockchain-Zertifikate können sowohl an juristische Personen wie an natürliche Personen ausgegeben werden. Akkreditierungsagenturen könnten somit auch ihre Akkreditierungszertifikate an eine Blockchain binden. Dadurch wäre es nicht nur möglich,

zu verifizieren, ob Studentin X tatsächlich ein Zertifikat von Hochschule Y erhalten hat, sondern auch, ob Hochschule Y von Akkreditierungsagentur Z zertifiziert wurde.

Wenn die beteiligten Institutionen ihre Zertifikate in einem öffentlichen Register zugänglich machen würden, könnte ein solches System genutzt werden, um sicherzustellen, dass der Bildungsanbieter, der das Zertifikat ausstellt, staatlich anerkannt ist oder dass ein Bildungsanbieter über spezifische Qualitätssiegel verfügt – dass zum Beispiel ein Anbieter von MBA-Abschlüssen tatsächlich durch EQUIS akkreditiert ist. Auf diese Weise wäre die Entwicklung mehrstufiger Verifizierungsverfahren möglich, mit denen Einzelpersonen mit einem einzigen Klick Folgendes überprüfen könnten:

» Abfrage bei der Institution, ob das Zertifikat tatsächlich dort ausgestellt wurde;
» die Qualität der Akkreditierung, die die Institution zu besitzen behauptet;
» Abfrage bei der Akkreditierungsagentur bzw. dem Akkreditierungsrat, ob der Institution tatsächlich das Zertifikat ausgestellt wurde;
» kraft welcher staatlichen Lizenz die Akkreditierungsagenturen ihre Akkreditierung verleihen;
» Abfrage bei der staatlichen Stelle oder zwischenstaatlichen Stelle (EQAR), ob der Akkreditierungsagentur tatsächlich eine Lizenz erteilt wurde.

Durch die leicht und automatisch herzustellende Transparenz von Qualifikationen würde eine solche Lösung es Titelmühlen erheblich erschweren, sich als seriöse Anbieter zu präsentieren.

4.3.8 AUTOMATISCHE ÜBERTRAGUNG UND AKKUMULIERUNG VON STUDIENLEISTUNGEN (CREDITS)

↖ AUTOMATISCHE ÜBERTRAGUNG UND AKKUMULIERUNG VON CREDITS

Eine automatische Übertragung und Akkumulierung von Studienleistungen (Credits) auf einer Blockchain setzt voraus, dass ein Netzwerk aus Organisationen, die Credits ausstellen, übertragen und akkumulieren, in koordinierter Form als Dezentralisierte Autonome Organisation (DAO) agiert. Bei einer DAO werden die Regeln der Organisation in einem Code als Smart Contract auf der Blockchain abgelegt; Änderungen an diesen Regeln werden über Abstimmungsverfahren vorgenommen, mit denen diese Smart Contracts aktualisiert werden und die ebenfalls auf der Blockchain stattfinden.

Eine DAO auf einer Blockchain repliziert (automatisiert) häufig die Strukturen und Prozesse einer bestehenden Organisation, im Rahmen derer eine Vielzahl von Parteien, die einander begrenzt vertrauen, auf der Grundlage gemeinsam vereinbarter Regeln komplexe Transaktionen aushandeln müssen. Ein solches Setting existiert zwischen Hochschulen im Hinblick auf die gegenseitige Anerkennung von Studienleistungen.

Mithilfe einer Blockchain könnten somit nach einstimmigem Beschluss aller an der DAO beteiligten Organisationen Vereinbarungen zur Übertragung von Credits als Smart Contracts formuliert werden, auf deren Grundlage Studienleistungen automatisch übertragen würden, sobald die Vertragsbedingungen erfüllt sind.

Dasselbe gilt für die Akkumulierung von Studienleistungen: Ein Smart Contract würde so programmiert werden, dass nach Erreichen bestimmter Credit-Ziele entsprechend der Prüfungsordnung der jeweiligen Hochschule automatisch ein Abschluss ausgestellt würde. So wäre sichergestellt, dass die Regeln zur Übertragung und Akkumulierung von Studienleistungen in allen Fällen auf berechenbare und reproduzierbare Weise zur Anwendung kommen.

4.3.9 TEILEN UND VERIFIZIEREN VON NACHWEISEN ERFAHRUNGSBASIERTER KOMPETENZEN

Erfahrungsbasierte Bildungsnachweise umfassen im Wesentlichen alle Nachweise von Bildungsinhalten oder Kompetenzen, die nicht im Nationalen Qualifikationsrahmen erfasst sind. Dazu zählen folglich

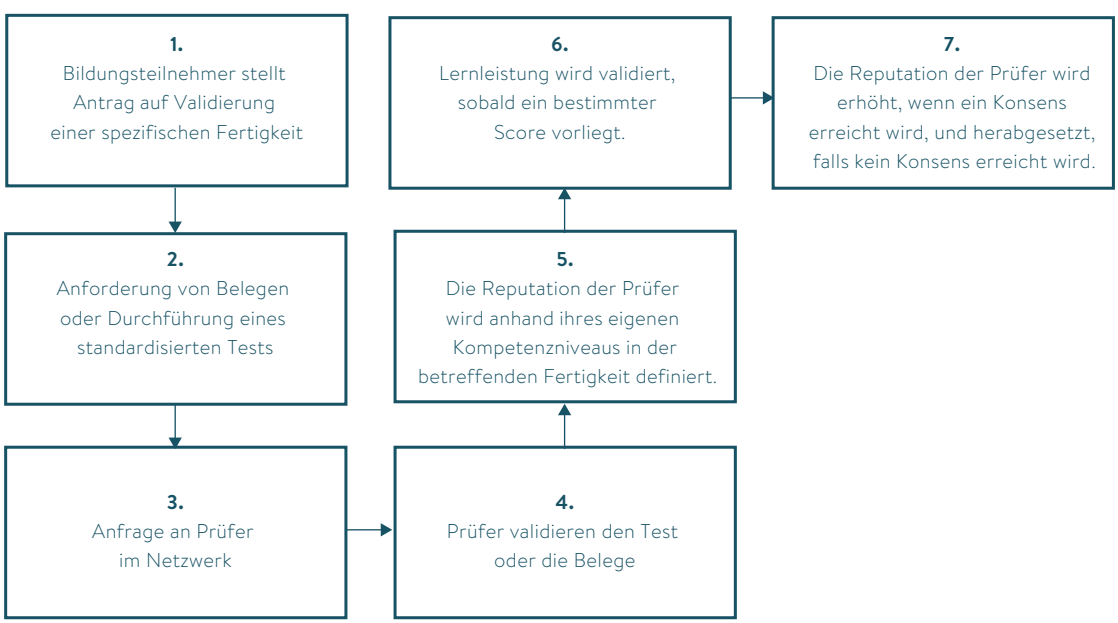
» Nachweise aus dem formalen Bildungssektor, die nach ausländischem Recht ausgestellt wurden und üblicherweise durch die ENIC-NARIC-Zentren beziehungsweise uni-assist verifiziert werden sowie
» alle Arten von Zertifikaten aus dem non-formalen und informellen Bildungssektor.

In diesem Fall würde nicht die ausstellende Institution die Daten auf die Blockchain laden, sondern die Bildungsteilnehmer selbst würden ihre eigenen Nachweise aus formaler, non-formaler oder informeller Bildung dort abspeichern. Bei der Weitergabe würde dann eine Blockchain zur sofortigen Überprüfung der Echtheit dieser Dokumente zum Einsatz kommen. Jeder hochgeladene Claim würde über die anderen Knoten der Blockchain validiert (durch die Überprüfung der Fakten des Claims). Sobald eine bestimmte Anzahl Nutzer die Richtigkeit des Claims bestätigt (und je nach Reputation der Nutzer, die den Claim verifizieren), würde dem Claim ein Glaubwürdigkeitswert (trust score) zugeordnet, der Ausdruck seiner Verifizierbarkeit ist.

↖ NACHWEISE

Ein idealtypischer Ablaufplan für ein derartiges System sähe folgendermaßen aus:

ABBILDUNG 26: ABLAUF FÜR DIE WEITERGABE UND VERIFIZIERUNG VON ERFAHRUNGSBASIERTEN ZERTIFIKATEN AUF EINER BLOCKCHAIN



Quelle: eigene Darstellung

4.3.10 ANALYSE

Marktreife

Die Technologie zur digitalen Beglaubigung von Bildungsnachweisen ist so weit fortgeschritten, dass mehrere Akteure, darunter die Regierung von Malta und die Universität von Nikosia, sie bereits heute in Echtzeit anwenden, wenngleich in begrenztem Umfang. Mehrere andere Regierungen sowie die Europäische Kommission untersuchen aktuell die Machbarkeit des Einsatzes eines Blockchain-basierten Beglaubigungssystems in verschiedenen Kontexten. In Deutschland entwickelt die Fraunhofer-Gesellschaft eine hybride PKI-Blockchain-Lösung für Zertifikate.

Darüber hinaus bieten bereits jetzt einige Firmen technische Lösungen, mit denen jedes Unternehmen eigene Blockchain-zertifizierte Nachweise ausstellen kann. Accredible und Gradbase zum Beispiel bieten jedem Nutzer die Möglichkeit, Blockchain-gesicherte Zertifikate auszustellen, während Learning Machine diese Dienstleistung momentan als Business-to-Business- und Business-to-Consumer-Lösung anbietet.

Einige Pilotimplementierungen zur Ausstellung von formalen Zertifikaten direkt auf der Blockchain befinden sich in einer sehr frühen Phase. So arbeitet die Universität von Maribor an einem Pilotprojekt zur Ausstellung von ECTS-Punkten auf einer Blockchain namens EduCTX; das MicroHE-Projekt untersucht den Nutzen von Blockchain für die Anerkennung von Mikroqualifikationen. Eine flächendeckende Einführung hängt in diesen Fällen davon ab, dass diese technischen Standards von einer großen Anzahl von Akteuren aufgegriffen werden; wahrscheinlich sind auch Anreize seitens des Gesetzgebers nötig.

Auch die Plattform Indorse hat ein kommerzielles Produkt zur Weitergabe und Verifizierung von erfahrungsbasierten Zertifikaten auf den Markt gebracht. Es ist anzunehmen, dass in den kommenden Jahren weitere Plattformen in diesen Markt vordringen werden.

Kosten- und Zeitersparnisse

Die vorgestellten Szenarien würden für alle beteiligten Parteien zu signifikanten Kostenersparnissen bei der Ausstellung und Verifizierung von Zertifikaten führen (insbesondere für Hochschulen, Studierende und Arbeitgeber), da eine sofortige und automatische Verifizierung möglich würde, für die die momentan verwendeten manuellen Verfahren nicht mehr nötig wären.

Sollten diese Lösungen flächendeckend zum Einsatz kommen, könnten sie zu erheblichen Kosten- und Zeitersparnissen bei den Hochschulen führen, da diese in die Lage versetzt würden, nicht nur die Authentizität von Zertifikaten automatisch zu verifizieren, sondern auch den Inhalt dieser Zertifikate. Da eine Automatisierung standardisierte Prozesse und Verfahren voraussetzt, sind diese Ersparnisse nach Ansicht der Autoren nur bei Vorliegen einer solchen Standardisierung erreichbar. Hinzu kommt, dass für dieses Szenario aufgrund der Komplexität der bestehenden Arrangements, die in ein Blockchain-basiertes System zu überführen wären, mit hohen finanziellen und zeitlichen Investitionen zu rechnen ist.

Voraussetzungen

Theoretisch kann jede Hochschule auch ohne allgemeinverbindliche Standards einen eigenen Beglaubigungsdienst einrichten, solange das Zertifikat einen Hinweis auf die Stelle enthält, die dessen Echtheit bestätigen kann. Gäbe es jedoch Hunderte oder gar Tausende verschiedener Verifizierungsformen, wäre es äußerst mühselig, für alle

eine automatische Verifizierung zu entwickeln. Vieles spricht deshalb dafür, sich auf gemeinsame technische Standards für die Beglaubigung zu verständigen. Learning Machine hat gemeinsam mit einigen Partnerorganisationen die Software Blockcerts entwickelt, die aus Open-Source-Bibliotheken, Tools und mobilen Apps besteht. Diese bilden ein dezentrales, auf Standards gestütztes und auf Nutzer ausgerichtetes System, das mittels Blockchain-Technologie ein Validierungsverfahren ohne Drittparteien ermöglicht. Ferner arbeitet die WCG Verifiable Claims Working Group an der Entwicklung eines globalen Standards für diese Claims.

Perspektiven

In Diskussionen mit Stakeholdern haben diese zu erkennen gegeben, dass sie einen Übergang zu sicheren digitalen Zertifikaten wünschen. In einem solchen Szenario wären PKI-basierte Zertifikate oder per Blockchain gesicherte Zertifikate die einzigen realistischen Optionen zur Digitalisierung von Bildungsnachweisen. Per Blockchain gesicherte Zertifikate stellen gegenüber PKI im Hinblick auf Unveränderbarkeit und die nicht vorhandene Notwendigkeit einer zentralen Ausstellungsinstanz eine erhebliche Weiterentwicklung dar. Solche Zertifikate dürften somit unter den Stakeholdern wahrscheinlich auf hohe Akzeptanz treffen und zum Einsatz kommen, solange keine künstlichen Barrieren (wie proprietäre Lösungen mit der Gefahr eines Vendor Lock-in) errichtet werden.

Auch mit der Entwicklung verifizierter institutioneller Identitäten könnte kurzfristig begonnen werden, falls etwa der Akkreditierungsrat die Einführung dieser Technologie beschlösse oder das European Quality Assurance Register for Higher Education (EQAR) seine Datenbank in ein Blockchain-basiertes System überführen würde. Unsere Workshops (siehe Abschnitt 4.9.1) haben ergeben, dass die automatische Akkumulierung und Übertragung von Studienleistungen einer der wünschenswertesten Anwendungsfälle für die Blockchain-Technologie wären. Allerdings handelt es sich hierbei dennoch um eine langfristige Perspektive, da zunächst in erheblichem Umfang neue Technologien in Form von Smart Contracts entwickelt, Governancestrukturen zwischen den beteiligten Organisationen geschaffen und die Regeln für die Übertragung und Akkumulierung von Studienleistungen für jedes Szenario verbindlich kodifiziert werden müssten.

Das Teilen und Verifizieren von erfahrungsbasierten Zertifikaten hat bessere Aussichten auf Implementierung mittels einer Blockchain, wenngleich die Akzeptanz stark von der Qualität der im Netzwerk vertretenen Prüfer und den damit verbundenen inhaltlichen Qualitätsstandards abhängen würde. Für den Fall, dass Agenturen, die non-formale und informelle Leistungen im Einklang mit den gesetzlichen Vorgaben validieren, diese Technologie einführen, ist mit einer schnellen Verbreitung und einem hohen Wirkungsgrad zu rechnen. Bis es soweit ist, könnten solche Dienstleistungen von Arbeitgebern genutzt werden, die für die Organisation ihrer eigenen Validierungsnetzwerke für Qualifikationen und Kompetenzen die Hilfe spezialisierter privater Validierungsagenturen in Anspruch nehmen könnten.

4.4 Software und Daten in Lehre und Studium dezentralisieren

4.4.1 HINTERGRUND UND AUSGANGSLAGE

Das Web 2.0 wird häufig als „social web“ bezeichnet. Es basiert auf Internetanwendungen, die es Menschen ermöglichen, zusammenzuarbeiten. Diese Zusammenarbeit

kann über ein soziales Netzwerk, über Tools zur Unternehmensproduktivität oder über Wissensplattformen wie Wikipedia stattfinden. Jede dieser Anwendungen wird von einer einzigen Firma oder Stiftung betrieben, die sowohl den Zugang zu den Daten kontrolliert als auch die physischen Server bereitstellt, auf denen die Daten gespeichert sind. Das bedeutet: Wer diese Plattformen benutzt, muss der zentralen Instanz vertrauen, dass die Daten nicht missbraucht werden. Insbesondere müssen Nutzer der zentralen Instanz im Hinblick darauf vertrauen,

VERTRAUEN AUF DATENSCHUTZ

» dass die Identität der Nutzer geprüft und gewährleistet wird, dass die Nutzer der Plattform tatsächlich die Personen sind, die sie zu sein behaupten, und dass die geposteten Inhalte real und seriös sind,
» dass die Plattform auf exakt die Weise betrieben wird, die den Nutzern in den Geschäftsbedingungen versprochen wird (Ehrlichkeit und Transparenz bei allen Transaktionen),
» dass gewährleistet ist, dass nicht-autorisierte Dritte die Daten weder lesen noch schreiben können (Datenschutz und Datensicherheit),
» dass die Betreiber ihr Monopol nicht dazu nutzen, ihre Dienstleistungen zu unfairen oder unverhältnismäßig hohen Preisen anzubieten,
» dass Nutzern die Möglichkeit zur Kommunikation gegeben wird; das heißt, dass alle Nutzer im Einklang mit dem Leitbild und den Regeln gleichberechtigt an der Plattform mitwirken können.

Die logische Konsequenz ist, dass diese zentralen Plattformen individuell oder kollektiv großen Schaden oder sogar Chaos anrichten können, wenn sie das in sie gesetzte Vertrauen missbrauchen. Daraus folgt, dass diese Plattformen die Macht besitzen, die Kontrolle über ihre Anwendungen zu nutzen oder zu missbrauchen und ein hohes Maß an Kontrolle über die Individuen und Gesellschaften in ihrem unmittelbaren Wirkungsbereich auszuüben. Dies wurde kürzlich exemplarisch daran deutlich, dass Datenschutzverletzungen bei Facebook zu Anhörungen im US-Kongress und einer Sonderanhörung im Europäischen Parlament geführt haben.

Im Bildungssektor sind zentralisierte Netzwerkanwendungen weit verbreitet und werden zu verschiedenen Zwecken verwendet, darunter

» Hochschulinformationssysteme,
» Lernmanagementsysteme,
» Echtzeit-Kommunikationstools wie Videokonferenzen und Chat-Anwendungen,
» kollaborative Office-Anwendungen, zum Beispiel Textverarbeitungs-, Tabellenkalkulations- oder Präsentationssoftware,
» Online-Archive und Bibliotheksanwendungen,
» durch Crowdsourcing generierte Referenzdatenbanken,
» soziale Netzwerke einschließlich beruflicher Netzwerke im Bildungsbereich.

Einige dieser Anwendungen werden von den Bildungseinrichtungen selbst auf ihren eigenen Servern betrieben, aber die meisten werden von externen und ausländischen Firmen betrieben und kontrolliert, bei denen die Bildungseinrichtungen eine Lizenz für die Nutzung erwerben. Es muss also darauf vertraut werden, dass diese Firmen die Daten ordnungsgemäß verwalten.

Diese Architektur bedeutet in der Regel,

NACHTEILE ZENTRALISIERTER DATEN-ARCHITEKTUREN

» dass Nutzer in unterschiedlichem Ausmaß die Kontrolle über ihre eigenen Daten an die Betreiberfirma abgeben müssen, damit die Anwendungen funktionieren, häufig auch als Gegenleistung für kostenlose Services;

- dass Nutzer keinerlei Kontrolle darüber haben, wo und wie ihre Daten gespeichert und gesichert werden;
- dass es schwierig ist, bei weltweit agierenden Unternehmen lokale Datenschutzstandards durchzusetzen und zu überwachen;
- dass Nutzer ihre Daten nicht ohne Weiteres von einem Anbieter zum anderen transferieren können;
- dass die Betreiberfirmen nach dem Modell Software-as-a-Service abrechnen können, das Nutzer an langfristige, kostenintensive Verträge bindet, die sich nach Abschluss nicht mehr leicht ändern lassen.

4.4.2 DEZENTRALISIERTE ANWENDUNGEN UND IHRE POTENZIALE

Dezentralisierte Anwendungen (dApps, siehe Abschnitt 3.6.4) erlauben Nutzern, frei zu wählen, bei welchen der leicht verfügbaren Clouddienste wie Dropbox oder BitTorrent sie ihre Daten speichern; die Anwendungen können die Daten mit dem Einverständnis der Nutzer auch lesen. Denn die App stellt sicher, dass alle Daten durchgängig signiert, verifiziert und verschlüsselt sind. Somit können Nutzer die Clouddienste wie Festplatten behandeln, problemlos den Anbieter wechseln oder die Daten einfach auf ihren eigenen Geräten behalten. Die dApp selbst speichert keine Daten, es gibt keine zentrale Instanz mehr, die Daten speichert oder die Software auf zentralen Servern ausführt. Da die Nutzer ihre eigene Speicherung mitbringen und Public-Key-Authentifizierung verwenden, müssen dezentralisierte Web-Anwendungen überhaupt nichts mehr speichern – und wenn sie gehackt werden, gibt es nichts, was gestohlen werden könnte. Außerdem können heute viele Web-Anwendungen so refaktoriert werden, dass alle Berechnungen auf der Client-Seite stattfinden. Somit ist es nicht mehr nötig, für die Anwendung einen gesonderten Server zu betreiben.

4.4.3 DEZENTRALISIERTE SOCIAL APPS FÜR DEN BILDUNGSBEREICH

Hochschulen können dApps nutzen, um ihren Lehrenden und Studierenden Software für Lehre und Studium zur Verfügung zu stellen, ohne das Hosting konfigurieren zu müssen und ohne Lock-in-Verträge mit proprietären Dienstleistern eingehen zu müssen.

Grundsätzlich kann jede im Bildungsbereich verwendete Anwendung wie Lernmanagementsysteme, Kollaborationssoftware oder Office-Software auf dezentralisierte Anwendungen umgestellt werden.

4.4.4 ANALYSE

Marktreife

Blockstack (blockstack.org) hat bereits eine Infrastruktur für dezentralisierte Apps auf den Markt gebracht und Einstiegs-Apps für die Zusammenarbeit im Büro wurden bereits entwickelt.[56] Im Bereich der dezentralisierten Anwendungen wird es wahrscheinlich in den kommenden Jahren zu einem hohen Maß an Innovation kommen, allerdings müssen dafür alle Apps von Grund auf neu geschrieben werden.

Kosten- und Zeitersparnisse

Die gesamten tatsächlichen Kosten einer dezentralisierten App-Infrastruktur wären wahrscheinlich höher als die einer zentralisierten App-Infrastruktur. Außerdem werden dezentralisierte Apps langsamer sein als zentralisierte Apps. In Zeiten von Multi-Core-Prozessoren in Handys und nahezu flächendeckend verfügbarem Breitband-Internet dürften diese Kosten jedoch kaum ins Gewicht fallen. Die Einführung dezentralisierter Apps würde außerdem bedeuten, dass die tatsächlichen Kosten

zum Betrieb der Apps (Elektrizität, Bandbreite, Speicherung) auf die Nutzer übergehen würden. Dies wären allerdings auch die einzigen Kosten, die entstehen, denn Servicegebühren oder Beiträge an Dritte wären nicht mehr zu zahlen. Die Kosten für die Nutzer dürften somit weit geringer sein als bei den gegenwärtigen Lösungen.

Voraussetzungen

Für echte dezentralisierte Apps werden aktive Entwickler-Communities benötigt, die diese Apps programmieren. Außerdem müssen Nutzer Zugang zu Geräten mit hoher Leistung und hoher Bandbreite haben.

Perspektiven

Es ist mit einer extrem hohen Nachfrage nach dezentralisierten Apps zu rechnen. Wirklich private und freie Bildungssoftware stellt für alle Akteure im Hochschulbereich einen großen Zugewinn dar. Ähnlich wie bei der Open-Source-Software, die auf anderen Gebieten flächendeckend eingeführt wurde, nachdem eine bestimmte Usability-Schwelle überschritten war, dürfte nach Einschätzung der Autoren auch die Einführung dezentralisierter Apps unausweichlich sein, sobald Software von ausreichender Qualität entwickelt wurde. Das Tempo der Einführung wird somit stark vom Vorhandensein von Anreizen zur Entwicklung solcher Software abhängen.

4.5 Studierendendaten in der Verwaltung minimieren

4.5.1 HINTERGRUND

Datenminimierung ist ein in Artikel 5 der DSGVO niedergelegtes Prinzip, nach dem personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden müssen. So kann gegen Unternehmen, die gegen diese Vorschriften verstoßen, eine Geldbuße in Höhe von bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes oder bis zu 20 Millionen Euro verhängt werden (je nachdem, welcher Wert der höhere ist). Zwar gelten für staatliche Einrichtungen bestimmte Ausnahmen von diesen gesetzlichen Regelungen, aber die Erwartungen der Öffentlichkeit an einen ordnungsgemäßen Umgang mit persönlichen Daten sind gegenüber der öffentlichen Hand besonders hoch.

↖ DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Hintergrund des Prinzips der Datenminimierung ist die Annahme, dass alle Datenspeichersysteme grundsätzlich Sicherheitslücken aufweisen und Ziel von Angriffen werden, weshalb die beste Verteidigung darin besteht, unnötige Daten gar nicht erst zu archivieren, um so eine Gefährdung des Datenschutzes und der Datensicherheit von vornherein zu minimieren. Somit ist es gleichzeitig ein Instrument zur Vereinfachung der Datenspeicherung und zur Senkung der damit verbundenen Kosten.

4.5.2 AUSGANGSLAGE

Innerhalb des Hochschulbildungssystems müssen sich Studierende[57] regelmäßig gegenüber verschiedenen Teilen des Systems identifizieren, zum Beispiel gegenüber der Hochschule wie auch gegenüber ihren verschiedenen Einheiten und mit ihr verbundenen Einrichtungen, etwa der Bibliothek oder dem Studentenwerk mit seinen angegliederten Einheiten wie Mensen und Cafeterien, Wohnheimen oder dem BAföG-Amt. Dies führt zunächst dazu, dass jeder Teil des Systems die Daten der Studierenden eigenständig erfassen und verwalten muss. Das heißt, die Identität der

Studierenden wird mehrfach verifiziert, was für das System erhebliche Verwaltungskosten verursacht und für die Studierenden einen erheblichen Zeitverlust, da sie ihre Unterlagen mehrfach einreichen müssen. Alternativ nutzen die Parteien eine einmalige Registrierung, bei der eine einzige Kopie der Daten eines Studierenden in einer zentralen Datenbank gespeichert und von allen Parteien einer Einrichtung genutzt wird (online zum Beispiel bei Single-Signon-Systemen).

In jedem Fall können Dutzende, wenn nicht Hunderte Personen Zugriff auf die persönlichen Daten der Studierenden haben und somit gegebenenfalls auf detaillierte Informationen zu ihrer finanziellen und sozialen Situation, ihrem Bildungsverlauf und eventuell sogar zu Aspekten ihrer Gesundheit und ihrer Religionszugehörigkeit. Damit diese Daten sicher bleiben, müssen nicht nur die Zugriffsrechte für all diese Personen verwaltet werden, es muss auch gewährleistet sein, dass ihre Endgeräte ebenfalls sicher und vor Hackerangriffen geschützt sind – eine Mammutaufgabe. So gab es in den letzten Jahren weltweit eine Flut von Fällen, bei denen die Systeme öffentlicher Einrichtungen kompromittiert wurden – das Spektrum reicht von Datenleaks über Datenverluste und Datenmissbrauch bis hin zu gehackten Daten.

↖
KOSTEN UND RISIKEN DER VERWALTUNG VON STUDIERENDENDATEN

Hochschulen kommen nicht darum herum, eine große Menge an Daten von den Studieninteressierten zu erheben, um die Zulassungsvoraussetzungen zu prüfen und festzustellen. Desgleichen generieren sie selbst große Mengen an neuen personenbezogenen Daten in Form zum Beispiel von Prüfungsdaten, Leistungsnachweisen und Abschlüssen. Dies führt zu:

» hohen Kosten für die Speicherung studentischer Daten und das Zugriffsmanagement;
» hohen Kosten für die Einhaltung gesetzlicher Vorschriften, insbesondere mit Blick auf die DSGVO;
» hohen Risiken durch Kosten, die durch potenzielle Verstöße gegen den Datenschutz und die Datensicherheit entstehen könnten.

Außerdem geben Bildungseinrichtungen die Daten von Studierenden nicht automatisch an andere Teile des Systems weiter, was dazu führt, dass Studierenden unnötige Bürokratie aufgebürdet wird, mehrere Zugriffspunkte auf ihre Daten geschaffen werden und sich das Gesamtrisiko eines Missbrauchs erhöht. Ein typisches Beispiel: Eine Studierende muss ihre Studienberechtigung nachweisen, indem sie dem Immatrikulationsbüro eine beglaubigte Kopie ihres Abiturzeugnisses übergibt; später muss sie eine weitere Kopie dieses Zeugnisses beim Prüfungsbüro einreichen, um zu den Prüfungen zugelassen zu werden.

Insgesamt schätzen die Autoren angesichts der Komplexität von möglichen Verteidigungsstrategien gegen Angriffe die Wahrscheinlichkeit als hoch ein, dass es zu erheblichen Datenschutzverletzungen bei den Studierendendaten kommen wird.

4.5.3 EINSATZ UND POTENZIAL DER BLOCKCHAIN

In diesem Szenario würden die Einrichtungen, die personenbezogene Daten von Studierenden benötigen, um ihren Anspruch auf bestimmte Dienstleistungen zu überprüfen, zunächst diese Daten prüfen. Dann würden sie eine Blockchain nutzen, um den Hash-Wert eines Zertifikats, das die Identität eines Studierenden und dessen Anspruch auf Dienstleistungen belegt, zu speichern und anschließend ebenfalls den Hash-Wert der vorgelegten Belege zu speichern. Anschließend könnte die Einrichtung alle gespeicherten Daten löschen, sodass keine Daten mehr gefährdet sind. Die Studierenden könnten ihre Identität durch Vorlage des Zertifikats nachweisen,

das im Abgleich mit dem Eintrag auf der Blockchain validiert werden könnte, ohne dass dafür die zugrundeliegenden Daten offengelegt werden müssten.

Im Ergebnis haben nur die Personen, die bei der Erstanmeldung für die Identifizierung von Studienbewerbern verantwortlich sind, Zugriff auf deren Daten. Da die übrigen Stellen nur wissen müssen, dass beziehungsweise welchen Anspruch auf Dienstleistungen ein Studierender hat, wird die Blockchain zur Erzeugung eines überprüfbaren, vertrauenswürdigen studentischen Identitätsnachweises genutzt. Damit ist es den anderen Teilen der Einrichtung und anderen Einrichtungen möglich, die Identität von Studierenden auch ohne Zugriff auf die zugrundeliegenden personenbezogenen Daten zu prüfen, die somit im Besitz der Studierenden bleiben. Dies bedeutet, dass die Einrichtung nicht länger ein komplexes System der Zugriffsverwaltung betreiben muss und nur noch die Sicherheit derjenigen Geräte und Netzwerke zu gewährleisten hat, die zur Ersterfassung der Daten verwendet werden. Dadurch würden erhebliche Ressourcen eingespart, die momentan für den Schutz des Netzwerks vor Datenschutzverletzungen, für die Weiterbildung der Beschäftigten in Datenschutzfragen und für die Verwaltung von Zugriffsrechten eingesetzt werden. Außerdem müssten Personen, die innerhalb der Einrichtung mit den Studierenden interagieren, nicht die Verantwortung für den Schutz sensibler personenbezogener Daten übernehmen, denn sie würden diese Daten gar nicht erst erhalten.

4.5.4 MANAGEMENT DER STUDIERENDENIDENTITÄT IM HOCHSCHULBILDUNGSSYSTEM

In diesem Anwendungsfall würde eine bestimmte Einheit innerhalb einer Hochschule damit beauftragt, die Identität von Studierenden zu bestimmen und ihnen anschließend einen Nachweis über diese Identität auszustellen, zum Beispiel in Form eines Studierendenausweises. Die zugrundeliegenden Daten, die zur Überprüfung der Identität der Studierenden verwendet wurden, würden danach gelöscht. Damit würde der Studierendenausweis selbst zum gültigen Nachweis des Anspruchs auf Dienstleistungen in allen Bereichen der Hochschule und des Hochschulsystems.

4.5.5 ANALYSE

Marktreife

Mehrere Firmen bringen zurzeit Blockchain-basierte Identitätsmanagement-Lösungen auf den Markt, die in diesem Szenario zum Einsatz kommen könnten. Momentan würde dies erfordern, dass die Hochschulen erheblichen technischen Aufwand betreiben müssten, um diese Systeme in ihre aktuellen Hochschulinformationssysteme zu integrieren.

Kosten- und Zeitersparnisse

Die Einführung Blockchain-basierter Identitätslösungen würde in jeder Hochschule, die diese Lösungen übernimmt, zu einer deutlichen Senkung der Kosten für die Einhaltung der gesetzlichen Datenschutzbestimmungen führen.

Voraussetzungen

Da Compliance-Aspekte im Hinblick auf die DSGVO eine wichtige Rolle bei diesem Szenario spielen, würde ein Zertifizierungssystem für Softwarelösungen die Einführung dieser Art von Lösungen sehr begünstigen. Außerdem gehen die meisten Implementierungen solcher Systeme pauschal davon aus, dass alle Nutzer ihre Smartphones oder Smartwatches für die Verwaltung ihrer Daten benutzen. Die Hochschulen müssten daher die Anschaffung dieser Geräte verlangen oder sie ihren Studierenden falls nötig zur Verfügung stellen.

Perspektiven

Nach Ansicht der Autoren ist nicht zu erwarten, dass Hochschulen solche Software selbst entwickeln. Die Daten der Studierenden werden normalerweise mithilfe von Software verwaltet, die von Anbietern von Hochschulinformationssystemen zur Verfügung gestellt wird. Sollten diese Anbieter eine Blockchain-basierte Lösung als Element ihrer Architektur einführen, würde diese mit hoher Wahrscheinlichkeit schnell übernommen. Aufgrund der technischen Herausforderungen ist jedoch mit einer Einführung eher mittel- bis langfristig zu rechnen.

4.6 Akademische Inhalte und Werke nachverfolgen

4.6.1 HINTERGRUND

Akademische Inhalte und Werke in Lehre und Forschung, mithin geistiges Eigentum (Intellectual Property, IP), nehmen in der strategischen Ausrichtung vieler Bildungseinrichtungen und insbesondere bei Hochschulen eine Schlüsselrolle ein. Dafür gibt es mehrere Gründe: Erstens unterstützt ein Großteil des von Hochschulen erzeugten geistigen Eigentums die eigene Lehr- und Forschungstätigkeit. Zweitens verfügen Hochschulen heute über eigene Kapazitäten für den Wissenstransfer zwischen Forschung, Wirtschaft und Gesellschaft. Drittens erzeugt die Forschung (und Innovation in der Bildung allgemein) neues Wissen und eine breite Grundlage für Innovation in Wissenschaft und Wirtschaft, die oft über Fachkonferenzen, Publikationen, Forschungskooperationen und Lehre, aber auch durch den Technologietransfer vermittelt wird. Dies befördert zukünftige kommerzielle oder staatliche Anwendungen. Aus diesem Grund wird die Leistung von Wissenschaftlern an Hochschulen hauptsächlich daran gemessen, wie viel neues geistiges Eigentum sie erzeugen und welchen Wert dieses geistige Eigentum hat. Dieser Wert wird gewöhnlich anhand von Indikatoren wie der Anzahl der Zitationen in wissenschaftlichen Publikationen gemessen.

Je nach Leitbild verfolgen Hochschulen eine Mischung aus unterschiedlichen Lizenzierungsstrategien. Grob lassen sich zwei Kategorien unterscheiden:

↖
OFFENE VS. GESCHLOSSENE LIZENZEN

- Mit einer *offenen Lizenz* verzichtet eine Einrichtung auf viele Urheberrechte an ihrem geistigen Eigentum, damit die allgemeine Öffentlichkeit die Erkenntnisse im öffentlichen Interesse nutzen kann.
- Mit einer *geschlossenen Lizenz* wird das geistige Eigentum geschützt, normalerweise in Form von Urheberrechten, Markenzeichen und/oder Patenten, um es auf diese Weise kommerziell nutzbar zu machen.

Im Rahmen des IP-Managements werden Ledgers (Bestandsbücher) verwendet, um

- festzuhalten, wann und von wem ein Werk zuerst erschaffen wurde (dies ist nötig zur Bestimmung der Urheber- und Inhaberschaft),
- Änderungen der Inhaberschaft oder Lizenzierung des geistigen Eigentums aufzuzeichnen,
- die Nutzung des geistigen Eigentums durch Dritte zu dokumentieren, meistens um Reputationszuweisung zu verfolgen oder Lizenzgebühren zu berechnen.

4.6.2 AUSGANGSLAGE

Gegenwärtig ist die Nachverfolgung von akademischen Inhalten und Werken ein kostspieliges Unterfangen, das von spezialisierten Anbietern durchgeführt wird, vor allem, wenn ein erhebliches geschäftliches Interesse daran besteht. Verwertungsgesellschaften überwachen die Nutzung von urheberrechtlich geschützten Musik- und Filmwerken; auf die Analyse wissenschaftlicher Daten spezialisierte Unternehmen messen die Zitationen von Artikeln – ein wichtiger Indikator für die Qualität wissenschaftlicher Forschung und den Fortschritt im Wissenschaftsbereich. Spezialisierte Kanzleien überwachen die Nutzung von Patenten, um entsprechende Lizenzgebühren zu erheben.

↖ ALTMETRICS

Aufgrund der Komplexität der Nachverfolgung von akademischen Inhalten und Werken ist es Personen, die ihre Werke im Eigenverlag veröffentlichen, trotz der steigenden Popularität von Altmetrics nur schwer möglich, deren Nutzung nachzuverfolgen und sich die Nutzung ihrer Inhalte und Werke zuschreiben oder vergüten zu lassen. Zum Beispiel wird die Wiederverwendung offener Bildungsressourcen allgemein gar nicht überwacht oder nur mithilfe äußerst einfacher Metriken mit begrenztem Nutzen.

Die meisten Firmen, die im Auftrag von Organisationen geistiges Eigentum verwalten, haben aufgrund der inhärenten Netzwerkeffekte im IP-Management eine Quasi-Monopolstellung in ihrer Branche erreicht. Dies hat in der Wissenschaft massive Kritik hervorgerufen: Die Firmen hätten zu große Macht über die Produktion und Nutzung geistigen Eigentums und missbrauchten diese Macht vor allem durch überzogene Lizenz- und Gebührenregelungen. Das bekannteste Beispiel für diese Kritik ist vielleicht die gegen Elsevier gerichtete „Cost of Knowledge"-Kampagne.[58] Die Open-Education-, Open-Science- und Open-Innovation-Bewegungen sind auch als Gegenbewegung zu den Geschäftspraktiken dieser Firmen entstanden.

4.6.3 EINSATZ UND POTENZIAL DER BLOCKCHAIN

In diesem Szenario würden Hochschulangehörige, die akademische Inhalte und Werke erschaffen, eine Blockchain nutzen, um das Datum der Veröffentlichung und das veröffentlichte Material notariell beurkunden zu lassen und dadurch einen Urheberrechtsanspruch zu schaffen. Außerdem könnte eine Blockchain dazu verwendet werden, die Nutzung dieses geistigen Eigentums nach der Veröffentlichung zu überwachen (mithilfe verschiedener Nutzungsmetriken, je nach Anwendungsfall).

↖ MITTLERINSTANZEN IM IP-MANAGEMENT

Aus struktureller Sicht ähnelt dieses Szenario stark den bereits bestehenden Datenbanken zur Verwaltung geistigen Eigentums. Bislang sind für das Urheberrechtsmanagement jedoch Mittlerinstanzen erforderlich, namentlich Verlage, deren Geschäftsmodell darin besteht, die Rechte Dritter zu verwerten und in gleichem Maße zu versuchen, die eigenen, von Dritten erworbenen Rechte zu verteidigen und zu schützen. Im Austausch für diese Dienstleistungen begrenzen die Verlage in der Regel die Möglichkeiten der Autoren, ihr eigenes geistiges Eigentum selbst zu nutzen, häufig in Form hoher Zugangskosten und Restriktionen hinsichtlich der Weitergabe und Nutzung des geistigen Eigentums. Dies erschwert die Verbreitung offener Lizenzmodelle im Vergleich zu geschlossenen Lizenzmodellen.

Mit dem Einsatz einer Blockchain entfällt die Notwendigkeit eines Mittlers bei der Verwaltung von Urheberrechten. In Verbindung mit den Möglichkeiten des Internets, eigene Inhalte jederzeit offen zu publizieren und zu verbreiten, birgt Blockchain ein erhebliches disruptives Potenzial im Hinblick auf die am Urheberrechtsmanagement beteiligten Modelle und Akteure.

4.6.4 BEGLAUBIGUNG VON AUTORENSCHAFTEN UND IP-RECHTEN

Bei diesem Anwendungsfall würden Personen, die akademische Inhalte und Werke erschaffen, das Datum der Veröffentlichung und einen Verweis auf die Publikation auf einer Blockchain ablegen. Auf diese Weise könnte jede Person ohne Einschaltung Dritter und mit geringem administrativen Aufwand einen überprüfbaren Autoren- und Urheberrechtsanspruch schaffen.

In der Regel würde dies dadurch geschehen, dass der Hash-Wert des publizierten Werks auf einer Blockchain archiviert wird. Dies beinhaltet auch die Möglichkeit, eine Autorenschaft beziehungsweise ein Urheberrecht anzumelden, ohne das zugrundeliegende Quellenmaterial öffentlich zugänglich zu machen, was das geltende Urheber- und Patentrecht grundlegend verändern würde.

4.6.5 NACHVERFOLGUNG DER NUTZUNG VON AKADEMISCHEN INHALTEN UND WERKEN

Statt lediglich die Veröffentlichung akademischer Inhalte und Werke zu dokumentieren, könnte eine Blockchain auch dazu verwendet werden, die Nutzung solchen geistigen Eigentums zu überwachen. Die Blockchain würde in diesem Fall normalerweise direkt von den Rechteinhabern oder ihren Vertretern verwaltet, ohne dass eine Mittlerinstanz beteiligt sein müsste. Auf diese Weise könnte die Nutzung und Wiederverwendung wissenschaftlicher Publikationen und/oder offener Bildungsressourcen sowie der Zitationen nachverfolgt werden. Ferner könnten Lizenzgebühren direkt von den Nutzern erhoben werden sowie diese Lizenzeinnahmen an die Rechteinhaber distribuiert werden.

Entscheidend ist, dass diese Anwendungen von den Rechteinhabern selbst durchgeführt werden könnten. Dadurch wäre es nicht länger nötig, Teile der Rechte an Dritte abzutreten.

4.6.6 ANALYSE

Marktreife

Technologisch betrachtet ist das Urheberrechtsmanagement mittels Blockchain längst Realität. Plattformen wie Bernstein (www.bernstein.io) bieten die notarielle Beurkundung von geistigem Eigentum.

Kosten- und Zeitersparnisse

Die notarielle Beurkundung von akademischen Inhalten und Werken auf Blockchains würde dieselben Kosten- und Zeitersparnisse mit sich bringen wie die im Abschnitt 4.3.10 beschriebenen. Die automatische Veröffentlichung, Überwachung und Vergütung von geistigem Eigentum mithilfe von Blockchains würde zu massiven Kostenersparnissen bei denjenigen führen, die dieses geistige Eigentum nutzen. Für Verlage und Firmen, die sich mit der Überwachung von Urheberrechten und Patenten beschäftigen, würde dies hingegen den Verlust einer maßgeblichen Einnahmequelle bedeuten.

Da die Kosten für Open Publishing sich per Definition nicht über Lizenzgebühren refinanzieren müssen, würde eine solch starke Preissenkung Anreize insbesondere für frei zugängliche Veröffentlichungen schaffen.

Voraussetzungen

Bei diesem Szenario würde eine spezielle Blockchain erzeugt, die es Hochschulangehörigen erlauben würde, (a) die Publikation ihrer Ressourcen öffentlich zu erklären

und einen Link zu diesen Ressourcen zu setzen und (b) zu erklären, welche anderen Ressourcen sie bei der Erschaffung ihres Materials verwendet haben. Die Hochschulangehörigen würden entsprechend der Intensität der Wiederverwendung ihrer Ressourcen mit Coins honoriert werden können.

In einem offenen Szenario könnten die Coins nicht ausgegeben werden, sondern würden dazu dienen, die Reputation eines Autors zu ermitteln. In einem geschlossenen Szenario hätten die Coins einen Geldwert und würden eine monetäre Vergütung nach sich ziehen.

Eine technisch verfeinerte Implementierung könnte Ressourcen automatisch scannen, um zu ermitteln, welcher Anteil anderer Ressourcen wiederverwendet wurde, und dies automatisch entsprechend honorieren.

Perspektiven

Für die notarielle Beurkundung von akademischen Inhalten und Werken wird eine sehr kurzfristige Umsetzungsperspektive prognostiziert, da die Technologie bereits vorhanden ist. Diese Anwendung bedeutet eine klare Weiterentwicklung der derzeit verwendeten Systeme und erfordert keinerlei rechtliche oder politische Änderungen, um vollumfänglich umgesetzt zu werden.

Überdies ist zu erwarten, dass viele Datenverarbeitungsgesellschaften ihre internen Verwendungs- und Wiederverwendungsdaten aus Gründen der Effizienz, Sicherheit und Unveränderbarkeit auf Blockchains verlagern.
Nach Einschätzung der Autoren ist die Dezentralisierung von Datenbanken an die Akteure allerdings nur mittel- bis langfristig wahrscheinlich und in hohem Maße von politischen Erwägungen abhängig. Die aktuellen Systeme zur Zitationsverfolgung und die darauf aufbauenden Konzepte wissenschaftlicher Performance sind tief im Hochschulsystem verankert. Die aufkommende Altmetrics-Bewegung stellt zwar etliche dieser Konventionen in Frage, befindet sich aber noch ganz am Anfang. Obwohl die Blockchain-Technologie also den Aufstieg von Altmetrics und die Demokratisierung der darauf basierenden Systeme befördern könnte, ist sie nicht der Hauptfaktor, der ihre Einführung ermöglicht.

4.7 Zahlungen und Mittelflüsse managen

4.7.1 HINTERGRUND UND AUSGANGSLAGE

Eine Zahlung ist nichts weiter als der Transfer von Geld von einer Partei zur anderen. Wie in den vorherigen Abschnitten erläutert, war vor der Erfindung von Blockchains für sichere digitale Zahlungen der Dienst eines vertrauenswürdigen Mittlers nötig, um dafür zu sorgen, dass das definitive Ledger (Bestandsbuch) den tatsächlichen Kontostand anzeigt. Dies erhöht die Komplexität der Transaktion und die anfallenden Kosten und/oder Gebühren des Mittlers erhöhen die Kosten jeder Transaktion. Komplexe finanzielle Transaktionen mit mehreren Parteien erfordern gegebenenfalls die Dienste mehrerer Mittler, was zu erheblichen administrativen, zeitlichen und finanziellen Mehrkosten für jede Form von finanzieller Transaktion führt. Einer der Hauptgründe, warum digitale Zahlungsmethoden die Barzahlung in vielen Ländern nicht ersetzen konnten, ist der doppelte Wunsch, dem Mittler keine Informationen anzuvertrauen und diese Mehrkosten nicht zu erzeugen.

In speziellen Fällen können die Kosten von Zahlungen so hoch sein, dass bestimmte Formen der Zahlung gar nicht erst stattfinden. So werden beispielsweise zentralisierte Zahlungssysteme generell nicht für Kleinstzahlungen verwendet.

Bildungsanbieter nutzen eine Vielzahl unterschiedlicher Finanzierungsmodelle, zum Beispiel leistungsbezogene Mittelzuweisungen, Globalbudgets, formelgestützte Budgets sowie Schul- oder Studiengebühren. Zusätzlich können gebührenzahlende Studierende selbst Leistungsvereinbarungen oder formelgestützten Mittelzuweisungen seitens ihrer Förderer unterliegen. Gemäß der Theorie der Eigentumsrechte und der Theorie der Transaktionskosten haben die Struktur der Eigentumsrechte sowie die Struktur und Höhe der Transaktionskosten einen Einfluss auf den Nutzen und Schaden der Akteure und somit auf ihre Entscheidungsfindung. Unter den gegebenen institutionellen Rahmenbedingungen entscheiden sich Akteure für diejenigen Formen der Ressourcennutzung und diejenigen Optionen im Eigentumsrecht, die ihren Nutzen maximieren. Diese Theorie erklärt auch, warum Innovationen in der Bildungsfinanzierung mitunter keine weite Verbreitung finden.

↖ **FINANZIERUNGSFORMEN IM DEUTSCHEN HOCHSCHULWESEN**

Für die Finanzierung von Hochschulen und Studierenden gibt es in Deutschland verschiedene institutionelle und individuelle Finanzierungsformen. Dazu zählen unter anderem:

- Grundfinanzierung: Haushaltsmittel der Länder;
- zusätzliche leistungsbezogene/formelgestützte Mittelzuweisungen nach Indikatoren wie Anzahl der Vollzeitstudierenden oder Anzahl der verliehenen Abschlüsse;
- staatliche Darlehen/Zuschüsse zu den Lebenshaltungskosten: BAföG (von den örtlichen Studentenwerken verwaltete Bundesmittel)
- Studienkredite: Darlehen der Kreditanstalt für Wiederaufbau (KfW) und privater Banken;
- Bildungskredit: Darlehen der KfW für Studierende in den letzten Jahren der Ausbildung;
- Deutschlandstipendium (die Hälfte der Förderung zahlen private Förderer, die andere Hälfte übernimmt der Bund);
- Stipendien von Stiftungen (Studienstiftung des Deutschen Volkes sowie den Parteien, Gewerkschaften, Kirchen und Arbeitgebern nahestehende öffentliche Begabtenförderwerke).

↖ **INEFFIZIENZ DER FINANZIERUNGSMODELLE**

Somit finden über das gesamte Bildungssystem hinweg täglich Millionen finanzielle Transaktionen statt, die von Banken und Finanzinstitutionen vermittelt und von staatlichen Institutionen unterstützt werden. Die Kosten pro Transaktion können je nach Komplexität und Höhe von wenigen Cents bis zu mehreren Tausend Euro reichen. Finanzierungsmodelle im Hochschulsystem können aus mehreren Gründen sehr ineffizient sein:

- Die Zahlungen können mit hohen Kosten verbunden sein. Kreditkarten- und Überweisungsgebühren können insbesondere für Studierende aus Drittweltländern unerschwinglich sein. Für Studierende mit Migrationshintergrund oder bestimmten religiösen Überzeugungen kann auch der Zugang zum Bankensystem ein Problem darstellen.
- Leistungsbezogene Finanzierungsmodelle, ob für Hochschulen oder Studierende, erzeugen hohe Verwaltungskosten für das Monitoring der Leistungen und die entsprechende Freigabe der Zahlungen sowie für die Verfolgung potenzieller Betrugs- und Missbrauchsfälle.

» Finanzierungsvereinbarungen für die Lehre beinhalten eine mehrjährige Bindung an Studienplätze und lassen sich nur mit großem Aufwand im Rahmen einer rechtlichen Vereinbarung kodifizieren. Trotzdem werden Finanzierungsbedingungen manchmal nach dem ursprünglichen Abschluss zum Nachteil der Studierenden und/oder der Hochschulen geändert.

4.7.2 EINSATZ UND POTENZIAL DER BLOCKCHAIN

Bei diesem Szenario würden Zahlungen und Mittelflüsse im Hochschulsystem über Blockchains abgewickelt – mithilfe von Fiat- oder Kryptowährungen. Möglich wäre dies beispielsweise für staatliche Mittelzuweisungen, die Zahlung von Studiengebühren oder Zahlungen an die Anbieter von Studieninhalten. Die Zahlungsformeln und -vereinbarungen würden direkt auf die Blockchain programmiert. So würden Zahlungen auf der Grundlage von Voreinstellungen freigegeben, die automatisch ausgelöst und überwacht würden.

Aus Sicht der Förderorganisationen (zum Beispiel staatliche Stellen) würde eine Reduzierung der Kosten bei der Verwaltung formelgestützter und leistungsbezogener Zuweisungsmodelle die Attraktivität dieser Modelle im Bildungsbereich steigern. Private Förderer wie Unternehmen und Nichtregierungsorganisationen wären auch eher bereit, sich an der Bildungsfinanzierung zu beteiligen, wenn mittels Blockchain eine bessere und kostenwirksamere Steuerung ihrer Investitionen gewährleistet wäre.

Schließlich würde die Kodifizierung von Vereinbarungen in Form von unveränderbaren Smart Contracts Fördergarantien für die gesamte Studiendauer bieten, indem die Fördermittel sicher auf einem Treuhandkonto abgelegt und anschließend nach vorgegebenen Kriterien freigegeben oder erstattet würden, wobei die Förderregeln nur durch einstimmigen Beschluss aller beteiligten Parteien geändert werden könnten.

4.7.3 ZAHLUNG VON STUDIENGEBÜHREN

In diesem Anwendungsfall entrichten die Studierenden die Gebühren über Blockchain-basierte Kryptowährungen.

4.7.4 STUDIENFÖRDERUNG

In diesem Anwendungsfall würden staatliche (oder private) Fördermittel den Studierenden als digitale „Gutscheine“ auf einer Blockchain zur Verfügung gestellt. Die Gutscheine könnten so programmiert sein, dass Teilzahlungen, gegebenenfalls auf Grundlage bestimmter Leistungskriterien wie Noten, entweder an die Studierenden selbst oder an die Bildungseinrichtung freigegeben werden.

4.7.5 LEISTUNGSBEZOGENE MITTELZUWEISUNG

In einem weiteren Anwendungsfall ließe sich dasselbe Konzept auch auf Zahlungen an Beschäftigte oder auf Mittelflüsse an Hochschulen anwenden.

Über Smart Contracts auf einer Blockchain könnten automatisch Anreize für Beschäftigte geschaffen werden, bestimmte Leistungsziele zu erreichen, zum Beispiel im Hinblick auf Publikationen, Benotung der Studierenden oder Transfer von geistigem Eigentum, sowie automatisch Anreize für Hochschulen geschaffen werden, bestimmte Leistungsziele zu erreichen, zum Beispiel im Hinblick auf Studierendenzahlen, Durchschnittsnoten oder Publikationen.

4.7.6 ANALYSE

Marktreife

Der Markteintritt Blockchain-basierter Zahlungen im Bildungsbereich ist auf niedriger Verwaltungsebene in Kürze zu erwarten. Mehrere Regierungen experimentieren derzeit mit Blockchains für staatliche Mittelzuweisungen und mehrere Universitäten (Beispiel: UNIC) akzeptieren bereits Zahlungen in Form von Kryptowährungen. Außerdem arbeiten mehrere Start-ups wie Woolf University, GLEDOS und Bitdegree an der Entwicklung von Plattformen zur Vernetzung von privatwirtschaftlichen Unternehmen, Einzelpersonen und Autoren sowie zur Abwicklung von Zahlungen untereinander auf Blockchains.

Kosten- und Zeitersparnisse

Kostenersparnisse ergeben sich hier vor allem aus der Reduzierung von Bankgebühren, die im Falle länderübergreifender Geldtransfers erhebliche Ausmaße annehmen können. Außerdem würde die Einführung Blockchain-basierter Smart Contracts einen großen Teil der Verwaltung in Form von formelgestützten Zuweisungen automatisieren und dadurch die administrativen Kosten solcher Systeme erheblich senken. In beiden Fällen verspricht die Blockchain-Technologie eine sofortige Zahlung, im Gegensatz zu den Verzögerungen, die heute aufgrund der Komplexität der Transaktionen häufig entstehen.

Voraussetzungen

Aus Sicht der Blockchain-Technologie unterstützt beispielsweise die Ethereum-Blockchain bereits jetzt eine solche Funktion. Benötigt würden für die Nutzung des Systems (a) eine Software zum einfachen Zusammenbauen und Hochladen der Smart Contracts auf die Blockchain sowie (b) die entsprechenden Datenquellen (etwa eine Datenbank mit den Noten der Studierenden), damit die Smart Contracts ermitteln können, ob die Vertragsbedingungen erfüllt sind. Bei vielen Implementierungen von Smart Contracts werden alle benötigten Datenquellen ebenfalls auf der Blockchain abgelegt, sodass alle Daten in demselben Maße vertrauenswürdig sind.

Perspektiven

Nach Ansicht der Autoren wird die Zahlung von Studiengebühren über Blockchains kurzfristig Realität werden. Allerdings ist eher nicht davon auszugehen, dass die Bildungseinrichtungen direkt Zahlungen in Kryptowährungen entgegennehmen; wahrscheinlicher ist, dass Hochschulen Überweisungen empfangen, die über Blockchain (zum Beispiel die Netzwerke Ripple oder Stellar) ermöglicht wurden und einen festen Wert im Form von Fiat-Währungen haben. Im öffentlichen Sektor wird die Einführung von auf Kryptowährungen basierenden Finanzierungsalgorithmen davon abhängen, ob der Bund die Blockchain-Technologie für interne Transaktionen nutzt, denn alle Bestimmungen zu regierungsinternen Finanztransfers werden auf der Ebene der Finanzministerien und Zentralbanken reguliert. Sollten der Bund oder ein Land Blockchains für interne Finanztransaktionen einführen, ist zu erwarten, dass diese Systeme in den kommenden Jahren allmählich immer weiter verfeinert und entsprechend den politischen Schwerpunktsetzungen Finanzierungsalgorithmen mit höherer Leistungsfähigkeit entwickelt werden. Im Privatsektor ist zu erwarten, dass Unternehmen, die als Clearingstelle für Bildungsinhalte fungieren (das heißt, Urheber, Lernende und Förderer miteinander vernetzen), auf kurze Sicht zunehmend zu Blockchain-basierten Zahlungen übergehen werden, da sich dadurch die Gebühren, die ansonsten für Banken und andere Finanzinstitutionen anfallen, deutlich reduzieren lassen.

4.8 Weitere Szenarien

Die bisher vorgestellten Szenarien wurden so eingeschätzt, dass sie Studierenden, Hochschulen und dem öffentlichen Sektor eindeutige potenzielle Vorteile bringen würden. Darüber hinaus wurden noch einige andere Szenarien berücksichtigt, deren Wirkung jedoch als gering eingeschätzt wurde – entweder weil ihre Auswirkungen das Lehren und Lernen nur am Rande berühren oder weil die Blockchain-Technologie zum jetzigen Zeitpunkt noch keinen eindeutigen Mehrwert bietet.

4.8.1 WAHLEN

Abstimmungen in Form von Wahlen finden im Hochschulbereich in zahlreichen Zusammenhängen statt, etwa bei der Wahl der Studierendenvertretung oder bei der Besetzung von bestimmten Stellen innerhalb einer Universität.

Mehrere Unternehmen und Non-Profits entwickeln zurzeit Blockchain-basierte Lösungen für Wahlen, da die Zwischenergebnisse mit Blockchain jederzeit exakt abrufbar sind und Wähler überprüfen können, ob ihre Stimmabgabe gezählt wurde. Diese Lösungen werden jedoch im Kontext von anspruchsvollen Umfragen mit hohen Sicherheitsanforderungen entwickelt; entsprechend kostspielig und komplex ist ihre Anwendung.

Bei solchen Abstimmungssystemen wird es zwar ab einem gewissen Punkt wahrscheinlich zu größenbedingten Kostenersparnissen kommen, die es erlauben, jedem Unternehmen zu geringen Kosten Voting-as-a-Service-Anwendungen zur Verfügung zu stellen, aber die Autoren denken nicht, dass der Bildungsbereich einen überzeugenden Anwendungsfall für solche Anwendungen darstellt.

4.8.2 DEZENTRALISIERTE AUTONOME ORGANISATIONEN

Bei diesem Szenario geht es im Grunde darum, die Blockchain-Technologie „für alles Mögliche“ zu nutzen oder Blockchain-Hochschulen zu erschaffen, bei denen sämtliche finanziellen, administrativen und organisatorischen Vorgänge an eine Blockchain geknüpft und, falls möglich, über Smart Contracts automatisiert werden.

Einem solchen Szenario liegt die Vorstellung zugrunde, dass, wenn Governance-Entscheidungen einmal getroffen und über eine Blockchain-basierte Abstimmung beschlossen sind, die gesamte Verwaltung im Grunde automatisch abläuft und nur minimale menschliche Intervention erfordert.

BitDegree und Woolf University haben beide ICOs auf den Weg gebracht, um diese Institutionen zu entwickeln. Die ersten Anwendungen beinhalten jedoch nur einen Bruchteil der vielen Hundert Vorgänge, die üblicherweise in einer Hochschule anfallen. Der Nachweis steht somit noch aus, ob die Technologie mit einem solchen Komplexitätsniveau zurechtkommt und dabei effizienter arbeitet als die bestehenden Systeme.

4.8.3 INTEGRATION IN DEN GESAMTEN FORSCHUNGSPROZESS

In der Scientific Community setzt sich zunehmend die Praxis durch, Fachzeitschriften bereits vor einer Veröffentlichung über Forschungsfrage, Hypothesen, Design und Analysestrategien eines geplanten Forschungsvorhabens zu informieren. Auf diese Weise sollen problematische Forschungsmethoden wie p-hacking oder die Nichtveröffentlichung von Daten von vornherein vermieden werden.

Blockchains bieten einen einfachen Weg, wissenschaftliche Studien vorab anzumelden, ohne dass es dafür einer Mittlerinstanz bedarf, und der Öffentlichkeit gleichzeitig vollen Zugang zu den Voranmeldedaten zu geben. Die Unveränderbarkeit von Blockchains ist in diesem Kontext besonders nützlich, da jede Änderung der Studienparameter als neuer Eintrag protokolliert werden muss, wodurch sichergestellt wird, dass der gesamte Lebenszyklus eines Forschungsprojekts nachvollzogen werden kann.

Die in Berlin ansässige Initiative Blockchain for Science nimmt den gesamten Forschungsprozess sowie die systemischen Implikationen des Einsatzes von Blockchain-Technologie im Wissenschaftssystem in den Blick.[59]

4.8.4 PRÜFUNGEN

Blockchain kann zur Verwaltung der Logistik von auf mehrere Standorte oder an allen Hochschulen gleichzeitig eingesetzten Prüfungen eingesetzt werden. Bestimmte Prüfungen müssen, an potenziell Hunderte von Prüfungszentren weltweit verteilt, zu exakt derselben Zeit freigegeben und dann zur vorgegebenen Zeit wieder beendet werden.

Hier könnten Smart Contracts dazu verwendet werden, einen selbstgesteuerten Vertrag zu erstellen, der die Prüfungen zu den vorgegebenen Zeiten freigibt und wieder schließt. Sie könnten auch mit Identitätssystemen verknüpft werden, um nur autorisierten Prüfungsteilnehmern Zugang zu den Prüfungsunterlagen zu gewähren.

4.9 Einschätzungen von Stakeholdern und Experten

4.9.1 DISKUSSIONEN MIT STAKEHOLDERN IN DEUTSCHLAND

Am 27. April 2018 fand in Berlin ein Stakeholder-Workshop statt, um die in diesem Kapitel vorgestellten Szenarien zu diskutieren. Zu den Teilnehmern gehörten Vertreter von Hochschulen, Experten für Blockchains und Zertifikate, Studierendenvertreter sowie Mitarbeiter der Auftragnehmer. Der folgende Abschnitt fasst die Meinungen der Teilnehmer dieses Workshops zusammen.

↖ **ATTRAKTIVITÄT(EN) DER BLOCKCHAIN-SZENARIEN**

Die Stakeholder waren sich weitgehend einig, dass alle identifizierten Probleme, zu deren Lösung Blockchain-Technologie beitragen könnte, in der deutschen Hochschullandschaft tatsächlich bestehen. Es gab jedoch erhebliche Diskussionen über die Zweckmäßigkeit von Blockchain-Lösungen für diese Probleme, da die Teilnehmer der Ansicht waren, dass nicht alle Beschränkungen von ausreichender Bedeutung sind, um die Kosten für eine solche Lösung zu tragen. In einer Rangliste der Anwendungsbereiche, die durch Abstimmung auf Seiten der Teilnehmer erstellt wurde, konnten wir drei Attraktivitäts-Kategorien ermitteln:

TABELLE 6: STAKEHOLDER-BEWERTUNG DER BLOCKCHAIN-ANWENDUNGSFÄLLE

STAKEHOLDER-BEWERTUNG DER ATTRAKTIVITÄT EINER BLOCKCHAIN-LÖSUNG	ANWENDUNGSBEREICH
HOHE ATTRAKTIVITÄT	Ausstellung beglaubigter Bildungsnachweise (Abschnitt 4.3.5)
	Verifizierung von Zertifikaten (Abschnitt 4.3.6)
	Automatische Übertragung und Akkumulierung von Studienleistungen (Credits) (Abschnitt 4.3.8)
MITTLERE ATTRAKTIVITÄT	Verifizierte digitale Identitäten (Abschnitt 4.3.7)
	Teilen und Verifizieren von Nachweisen erfahrungsbasierter Kompetenzen (Abschnitt 4.3.9)
	Dezentralisierte Social Apps für den Bildungsbereich (Abschnitt 4.4.3)
	Management der Studierendenidentität im Hochschulbildungssystem (Abschnitt 4.5.4)
	Studienförderung (Abschnitt 4.7.4)
NIEDRIGE ATTRAKTIVITÄT	Beglaubigung von Autorenschaften und IP-Rechten (Abschnitt 4.6.4)
	Nachverfolgung der Nutzung von akademischen Inhalten und Werken (Abschnitt 4.6.5)
	Zahlung von Studiengebühren (Abschnitt 4.7.3)
	Leistungsbezogene Mittelzuweisung (Abschnitt 4.7.5)

Quelle: Eigene Datenerhebung, Stakeholder-Workshop am 27. April 2018 in Berlin

↖ **BARRIEREN IN DER IMPLEMENTIERUNG**

Die mit hoher Attraktivität ausgewiesenen Einsatzbereiche entsprechen den Erwartungen, da es sich hierbei um die derzeit ausgereiftesten Anwendungen der Blockchain-Technologie handelt. Innerhalb der wenig attraktiven Einsatzbereiche entspricht die geringe Erwünschtheit des Einsatzes für Zahlungen dem öffentlichen Fördermodell des deutschen Bildungswesens, das ohne größere Strukturveränderungen wenig Raum für solche Innovationen lassen würde. Die geringe Erwünschtheit von IP-verknüpften Lösungen entspricht jedoch nicht unserer Nutzenanalyse oder der Literatur, zum Beispiel aus dem Open-Education-Bereich. Während wir bei allen anderen Anwendungsfällen zu dem Schluss kommen, dass diese Aufstellung im Großen und Ganzen das Spektrum der aktuell vertretenen Expertenmeinungen widerspiegelt, vermuten wir, dass die geringe Erwünschtheit dieser genannten einzelnen Anwendungsfälle damit zusammenhängt, dass an unserem Workshop keine oder nur einzelne Personen teilnahmen, die sich täglich mit diesen Themen beschäftigen.

Der Workshop befasste sich weiterhin intensiv mit der kritischen Bewertung von Lösungsvorschlägen und der Frage, ob Blockchain eine signifikante Verbesserung gegenüber aktuellen Lösungen bieten würde. Während jedes Szenario separat diskutiert wurde mit dem Ziel, eine jeweils eigene SWOT-Analyse bereitzustellen, stellten wir fest, dass in allen Szenarien ähnliche Bedenken geäußert wurden, die hier zusammengefasst werden:

Technologische Faktoren (beinhalten Zweifel am technischen Design):

» Sicherheit: Mehrere Teilnehmer äußerten Bedenken, ob Blockchains wirklich so unhackbar sind wie behauptet und ob falsch implementierte Blockchains ein falsches Sicherheitsgefühl erzeugen könnten. Sie äußerten auch Bedenken, dass Blockchains nicht resistent gegen Social-Engineering-Angriffe sein könnten und solche Angriffe im Falle eines verstärkten Vertrauens in die Technologie zur Speicherung sensibler Daten effektiver wären.
» Effizienz: Teilnehmer zeigten sich insbesondere besorgt hinsichtlich der Energieeffizienz von Blockchains, wobei sich viele Teilnehmer auf den Energiebedarf der Bitcoin-Blockchain sowie auf die Realisierbarkeit großer Allzweck-Blockchains mit ihrem Speicherbedarf bezogen.
» Komplexität: Die Teilnehmer wiesen auf die Komplexität von Blockchain in Bezug auf die Softwareentwicklung sowie die Komplexität der zugrundeliegenden Konzepte und die Schwierigkeit des Verständnisses hin. Die Teilnehmer befürchteten, dass diese Komplexität die Kosten für Entwicklung und Schulung derart erhöhen würde, dass die Implementierung hinfällig würde.
» Unveränderbarkeit: Die Teilnehmer haben mehrere Fälle aufgeworfen, in denen eine Unveränderbarkeit nicht wünschenswert sein könnte. Dazu gehörten Szenarien im Zusammenhang mit der Ausübung des Rechts auf Löschung gemäß der DSGVO, die Folgen kompromittierter Benutzeridentitäten im Falle einer unveränderlichen Blockchain und das Potenzial, dass auch die Aktivitäten schlechter Akteure in der Blockchain unveränderlich sind.

Institutionelle Faktoren (umfassen Bedenken aufgrund der Governance-Struktur des Hochschulbildungssystems und der Managementsysteme innerhalb von Hochschulen):

» Konsensbildung: Die Workshopteilnehmer äußerten erhebliche Zweifel an der Idee, Konsensbildung in Blockchains auszulagern, da dies als eine mögliche Beeinträchtigung der institutionellen Autonomie angesehen wurde. So wurde zwar das Einsatzszenario der automatischen Übertragung und Akkumulation von Credits als das wünschenswerteste angesehen, gleichzeitig wurde dessen freiwillige Umsetzung auch als höchst unwahrscheinlich angesehen.
» Vertrauen und Dezentralisierung: Die Teilnehmer bewerteten Dezentralisierung differenziert. Während die Dezentralisierung weg von Konzernen wie Google und Facebook als positiv bewertet wurde, bestand kein Konsens über andere zentrale vermittelnde Instanzen wie akademische Verlage, Anbieter von Studierendeninformationssystemen und Anbieter von Lernmanagementsystemen. Darüber hinaus hielten es die Teilnehmer im Allgemeinen nicht für notwendig, Hochschulen und Regierungen als zentrale Behörden zu ersetzen, zum Beispiel im Hinblick auf die Überprüfung von Zertifikaten, da diese als vertrauenswürdige Akteure angesehen werden.
» Institutionelle Trägheit: Die Teilnehmer waren sich einig, dass deutliche inkrementelle Verbesserungen gegenüber den derzeitigen eingesetzten Technologien für Institutionen für sich genommen kein hinreichender Grund sind, Blockchain-Technologien einzusetzen. Die Nachteile der derzeitigen Systeme wirken sich in der Regel nicht unmittelbar auf die institutionellen Leistungskennzahlen aus, insbesondere nicht bei vollständig öffentlich geförderten Einrichtungen. Der Einsatz von Blockchain würde daher weitere Anreize erfordern, einschließlich der Vereinfachung der Implementierung, der Ausbildung, der Finanzierung und insbesondere der Rechtsvorschriften und der Normung.

4.9.2 INTERVIEWS MIT INTERNATIONALEN EXPERTEN

Die Perspektiven und Beiträge der deutschen Stakeholder-Community wurden durch Experteninterviews ergänzt, um eine internationale Perspektive auf die Entwicklung der Blockchain-Technologie im Hochschulbildungsbereich („Blockchain in Education") zu erhalten. Es wurden Interviews mit den folgenden Experten geführt, die auf der Grundlage ausgewählt wurden, dass (a) sie alle aktiv an der Umsetzung von Projekten im Bereich Blockchain in Education beteiligt sind, (b) sie alle regelmäßig mit Regierungen und Hochschulen zusammenarbeiten und (c) alle auf internationaler Ebene die Entwicklungen im Bereich der Blockchain in Education verfolgen:

» Dr. Joshua Broggi, Gründer und Direktor von Woolf; Faculty of Philosophy at Wolfson College, University of Oxford; Gastdozent, Institut für Philosophie, Humboldt-Universität zu Berlin.
» Dr. Perrine de Coetlogon, Ministere de l'Enseignement Superieur, de la Recherche et de l'Innovation sowie Head of Blockchain4Edu, University of Lille.
» Marloes Pomp, Dutch Blockchain Coalition.
» Alex Grech, Berater, Ministry of Education and Employment in Malta, und Leiter der Malta Blockchain certification pilots.
» Dr. Natalie Smolenski, Vice President Learning Machine.

Die Interviews basierten auf einem semi-strukturierten Fragebogen in den folgenden Kategorien. Alle in diesem Abschnitt geäußerten Ansichten sind die der Experten.

Foresight: Welche Aktivitäten im Bereich Blockchain in Education werden sich in den nächsten drei Jahren hauptsächlich entfalten?

↖ **KURZFRISTIGE ANWENDUNGSSZENARIEN**

» Alle Experten sind sich einig, dass in den nächsten drei Jahren die *Zertifizierung von Abschlüssen, Fähigkeiten und Kompetenzen* und open badges auf der Blockchain, die zwischen den Hochschulen beziehungsweise Bildungseinrichtungen geteilt und den Studierenden, aber auch Arbeitgebern und den Bürgern zugänglich gemacht werden, die Hauptaktivität sein wird. Die EU hat bereits ein Blockchain-gesichertes Element für den Europass angekündigt, während in Malta und Belgien Pilotprojekte auf nationaler Ebene laufen.

» *RegTech* – das heißt, der Einsatz von Technologie, um regulatorische Verfahren auf eine Blockchain zu übertragen – ist bereits klar im Bereich des Möglichen. Hochkonforme und hochautomatisierte Verfahren können in die Blockchain migriert werden, wodurch sich das Risiko von Verstößen gegen entsprechend kodierte Regulierungen deutlich reduziert.

» Blockchain-Technologie wird auch bei der *Lizenzierung von Open Education Ressources (OER)* eingesetzt, um die Rechte der Autoren zu zertifizieren und um den Mix oder Remix von solchen Inhalten nachzuverfolgen, die das Herzstück von Kursen und Lehrveranstaltungen bilden.

Weitere Entwicklung der Blockchain-Technologie

↖ **RESSOURCENEFFIZIENZ**

» Die Auswirkungen der DSGVO werden wahrscheinlich zu einer Reihe von technologischen Upgrades für verschiedene Blockchains und zur Schaffung von *DSGVO-konformen Blockchains* führen.
» Außerdem werden wahrscheinlich verschiedene Ansätze zur Lösung der ursprünglichen Ressourceneffizienzprobleme im Zusammenhang mit Blockchains der ersten Stunde wie Bitcoin zur Einsatzreife gebracht.

» Ein Beispiel für eine solche Blockchain ist Hyperledger, das im Gegensatz zu Ethereum auf Unternehmensebene eingesetzt werden kann. Es hat die richtigen Protokolle, um hohe Volumina und Komplexität von Transaktionen zu bewältigen, im Gegensatz zu Cloud-Servern. Hyperledger ist eine globale Kooperation, die von der Linux Foundation getragen wird, darunter sind führende Unternehmen aus den Bereichen Finanzen, Bankwesen, IoT, Supply Chain, Fertigung und Technologie. Es ist auch eine Open-Source-Kooperation, da jeder die Protokolle nutzen kann; es wurde geschaffen, um branchenübergreifende Blockchain-Technologien voranzutreiben, und ermöglicht interessante Projekte wie die Sovrin-Initiative[60] - ein dezentralisiertes globales öffentliches Versorgungsunternehmen für selbstbestimmte Identität.

Gesellschaftliches Nutzenversprechen von Blockchains

» Konzepte wie Unveränderlichkeit und Transparenz bedeuten für verschiedene Menschen unterschiedliche Dinge und es wird zu Interessenkonflikten kommen, sobald sich die Nuancen der Blockchain entfalten. Es gilt, den Kern der Prozesse zu erfassen – und dabei die Effizienzgewinne zu prüfen, die die Blockchain diesen Prozessen bringen kann.
» Durch die Dezentralisierung profitieren Institutionen von ihren eigenen Alumni, die in die Welt gehen und Markenbotschafter werden. Da auf der öffentlichen Blockchain beglaubigte Zertifikate manipulationssicher sind, schützen sie auch den Ruf der Marke der jeweiligen Institution. (Derzeit behaupten erstaunlich viele Leute auf LinkedIn, in Harvard gewesen zu sein!)
» Ein weiteres Beispiel für einen Interessenkonflikt ist der Fall, dass Absolventen eine schlechte Note nicht ihrem zukünftigen Arbeitgeber mitteilen wollen, auch wenn Arbeitgeber und Hochschule ein Interesse daran haben. Wir müssen also von vornherein entscheiden, wer über das Bildungszertifikat verfügt. Die einfachste Möglichkeit besteht darin, Zertifikate dem Empfänger – dem Lernenden – zuzuschreiben. Es läge dann an ihm, zu entscheiden, mit wem welche Elemente der lebenslang gesammelten Zertifikate geteilt werden.
» Für viele private Innovatoren hat Blockchain zunächst einen materiellen Wert ohne Zusammenhang mit dem sogenannten Nutzenversprechen der Blockchain. Die privaten Innovatoren, die Blockchain-Geschäftsmodelle entwickeln, die es auch in zehn Jahren noch geben wird, bauen die Unternehmen um ein soziales Nutzenversprechen herum auf, für das die Menschen auch bereit sind zu zahlen.

Die Rolle des Staates und der Regierung

» Entscheidungsträger nehmen das *Gesamtbild mit dem Datenschutz*, dem Schutz der Bürgerrechte und der Sicherheit in den Blick: Unter diesen Umständen ist der Nutzen von Blockchains vielfältig. Die Vorgabe der DSGVO von privacy by design and default wird von öffentlichen Blockchains erfüllt. Jedoch wurde die DSGVO zu einer Zeit konzipiert, als Blockchain-Lösungen noch nicht in Erwägung gezogen wurden. Informationen wurden als leicht löschbar angesehen. Das Recht auf Vergessen muss nun gegen das Recht zur Datenspeicherung abgewogen werden.
» Im öffentlichen Sektor könnten gegenüber dem privaten Sektor die *Effizienzgewinne* und Vorteile des Einsatzes von Blockchains größer sein. Zugleich existiert ein potenzieller Nutzen für die Allgemeinheit, der sich beispielsweise aus der Nutzung der Blockchain für selbstbestimmte Identitätsprojekte wie digitale Reisepässe ergibt, die von den Bürgern mitgeführt und die auf der Grundlage bestimmter Bedingungen durch Smart Contracts verwaltet und widerrufen werden können. Politische Entscheidungsträger sind wahrscheinlich aufgeschlossen gegenüber

↖ DER STAAT ALS KUNDE DER BLOCKCHAIN

Initiativen im Bereich Blockchain in Education, wenn diese sich an gemeinsamen staatlichen Interessen ausrichten.

- Die Politik muss sich aber auch des *Misstrauens der Bürger* bewusst sein: Es gibt grundlegende Auseinandersetzungen über die Fragen, welche Daten überhaupt erfassen werden sollen und wie das Interesse der Allgemeinheit gegen die Interessen der einzelnen Bürger abgewogen werden kann.
- Für wissenschaftliche Einrichtungen wie Hochschulen, Bibliotheken und Forschungszentren bietet die Unveränderlichkeit der Blockchain eine Möglichkeit, den *wissenschaftlichen und kulturellen Fortschritt* eindeutig zu erfassen – eine Grundlage für die meisten liberalen Demokratien.
- Der Staat hat eine *Funktion als Regulierer, aber auch als Abnehmer* der Blockchain-Technologie – er sollte erkennen, dass es Möglichkeiten gibt, die Bereitstellung öffentlicher Güter durch Blockchain zu verbessern.

DER STAAT ALS REGULIERER

- Die Rolle der Regierung besteht auch darin, die Wissenschaftler bei der *Koordinierung der Forschungsinteressen* zum Wohle der Allgemeinheit zu unterstützen: Auch private Netzwerke werden von dieser Forschung profitieren. Wenn nicht, besteht die Gefahr, dass sich Blockchain-Anwendungen nur aus rein privatem Gewinnstreben heraus entwickeln. Die Netzwerke müssen sich zusammenschließen: Die Mittel werden dann dazu verwendet, die Blockchain-Initiativen zu bündeln und gezielt Know-how in bestimmten Bereichen zu entwickeln.
- Es sollte eine Verpflichtung auf Prinzipien der offenen Standards bestehen. Wir müssen innovativ sein, aber es müssen einige Schutzvorkehrungen getroffen werden, um sicherzustellen, dass wir eine *soziale Infrastruktur für die Allgemeinheit* aufbauen. So wie das HTTP-IP-Protokoll für das Internet als öffentliches Gut entwickelt wurde, müssen wir das Konzept der offenen Standards für die Blockchain unterstützen.

Risiken des Einsatzes von Blockchain in der Hochschulbildung

- Es gibt *zahlreiche Akteure mit zweifelhaften Absichten* im Blockchain-Bereich, die der Technologie unweigerlich einen schlechten Ruf verleihen: Im Bewusstsein der Bevölkerung steht die Blockchain derzeit für Kryptowährungen, Spamming und privaten finanziellen Gewinn.

VERMEIDUNG ZWEIFELHAFTER BLOCKCHAINS

- Die Komplexität von Blockchain bedeutet, dass die Gefahr besteht, dass die Blockchain auf die falschen Prozesse angewendet wird, dass sie *ineffizient* auf große Projekte angewendet wird, die zu Verschwendung führen, oder dass sie dazu benutzt wird, die Verbraucher zu betrügen. All diese Bedrohungen können durch Marktinformationsmaßnahmen wie Ausbildung und Zertifizierung angegangen werden.
- Es gibt *Umweltaspekte*, die es zu berücksichtigen gilt. Im Bildungssektor gibt es Bedenken hinsichtlich der Energiekosten einer einzigen Transaktion in der Bitcoin-Blockchain.
- Die Hauptbedrohung ist die Balkanisierung – *keine Interoperabilität*, keine Möglichkeit der Überprüfung von Berechtigungsnachweisen, wenig Benutzerfreundlichkeit. Nutzer sollten in der Lage sein, ihre Daten zu besitzen, sie überall hin mitzunehmen und zu überprüfen.
- Schließlich bedeutet ein erfolgreicher weitreichender Einsatz von Blockchain-Technologie, dass sich der *Spielraum für menschliches Ermessen* verkleinert. Es bedarf einer sehr sorgfältigen Architektur: zum Beispiel, um sicherzustellen, dass sich bei Änderungen einer Policy die Prozesse, die diese Policy unterstützen, sofort ändern.

Kapitelendnoten

53 Nähere Informationen hier: http://uni-goettingen.de/de/576086.html, abgerufen am 29.05.2019.

54 Nähere Informationen unter https://www.groningendeclaration.org, abgerufen am 29.05.2019.

55 Weitere Informationen zu Titel- und Akkreditierungsmühlen siehe https://www.eqar.eu/kb/accreditation-mills/ abgerufen am 29.05.2019

56 Siehe https://blockstack.org, abgerufen am 29.05.2019.

57 Der Fokus liegt hier auf der Verwaltung von Studierendendaten, da der Datenschutzbedarf für Studierende nach Auffassung der Autoren höher ist als für die Beschäftigten einer Hochschule. Für Letztere besteht ein öffentliches Interesse an der Publikation von Lebensläufen, Qualifikationen, Erfahrungs- und Leistungsdaten, damit informierte Auswahlentscheidungen getroffen werden können. Somit gibt es hier eine geringere Notwendigkeit für Blockchain-basierte Lösungen.

58 Siehe http://thecostofknowledge.com, abgerufen am 29.05.2019

59 Weitere Informationen unter https://www.blockchainforscience.com/, abgerufen am 29.05.2019.

60 Weitere Informationen unter https://sovrin.org, abgerufen am 29.05.2019.

ANHANG

Literaturverzeichnis

Abraham, R. (2018). Can hashgraph succeed blockchain as the technology of choice for cryptocurrencies? Abgerufen am 29.05.2019 von http://www.thehindu.com/sci-tech/technology/can-hashgraph-succeed-blockchain-as-the-technology-of-choice-for-cryptocurrencies/article23348176.ece.

Acheson, N. (2018). How to Make a Paper Bitcoin Wallet, in: Coindesk. Abgerufen am 29.05.2019 von https://www.coindesk.com/information/paper-Wallet-tutorial/.

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., Tomamiche, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. arXiv:1710.10377v1. Abgerufen am 29.05.2019 von https://arxiv.org/pdf/1710.10377.pdf.

Ali, M., Shea, R., Nelson, J., Freedman, M. J. (2017). Blockstack: A New Internet for Decentralized Applications. Abgerufen am 29.05.2019 von https://blockstack.org/whitepaper.pdf.

Antonopoulos, A. (2017). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. UK: O'Reilly.

AXA (2017). AXA goes blockchain with fizzy. Abgerufen am 29.05.2019 von https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy.

Baird, L. (2016). The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. Abgerufen am 29.05.2019 von http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf.

Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. Abgerufen am 29.05.2019 von https://eprint.iacr.org/2014/452.pdf.

Beutelspacher, A., Neumann, H., Schwarzpaul, T. (2005). Kryptografie in Theorie und Praxis. Wiesbaden: Vieweg+Teubner Verlag.

Bevand, M. (2016). Bitcoin Mining is Not Wasteful. Abgerufen am 29.05.2019 von http://blog.zorinaq.com/bitcoin-mining-is-not-wasteful/.

Biederbeck, M. (2016). Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen. Abgerufen am 29.05.2019 von https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde.

Bitcoin.de (Internetseite). Wallet-Apps. Abgerufen am 29.05.2019 von https://bitcoin.org/de/waehlen-sie-ihre-Wallet.

Bitcoin Wiki (Internetseite). Full node. Abgerufen am 29.05.2019 von https://en.bitcoin.it/wiki/Full_node.

BitInfoCharts (Internetseite). Bitcoin (BTC) Statistiken und Informationen. Abgerufen am 29.05.2019 von https://bitinfocharts.com/de/bitcoin/.

Blockchain.com (Internetseite). Blockchain Size. Abgerufen am 28.05.2019 von https://www.blockchain.com/sl/charts/blocks-size.

Blockchain.com (Internetseite). Confirmed Transactions Per Day. Abgerufen am 28.05.2019 von https://www.blockchain.com/charts/n-transactions?timespan=all.

Blockchain.com (Internetseite). Last 50 blocks. Abgerufen am 28.05.2019 von https://chaindex.com/blockchain/

Blockchain.info (Internetseite). Statistiken zur Bitcoin-Blockchain. Abgerufen am 29.05.2019 von https://blockchain.info/stats.

Blockchain Bundesverband (2018). Blockchain, data protection, and the GDPR. Abgerufen am 29.05.2019 von https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf.

Bundesministerium für Arbeit und Soziales (2016). Weißbuch Arbeiten 4.0. Abgerufen am 29.05.2019 von https://www.bmas.de/DE/Service/Medien/Publikationen/a883-weissbuch.html.

Bundesamt für Sicherheit in der Informationstechnik (Internetseite). IT-Grundschutz Glossar und Begriffsdefinitionen. Abgerufen am 29.05.2019 von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

Bundesamt für Sicherheit in der Informationstechnik (Internetseite). PKI und Digitale Signatur. Abgerufen am 29.05.2019 von https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/Grundlagenwissen/DigitaleSignatur/digitale_signatur_node.html.

Burst-Coin (Internetseite). Proof of Capacity. Abgerufen am 29.05.2019 von https://www.burst-coin.org/proof-of-capacity.

Buterin, V., et al. (Internetseite). A Next-Generation Smart Contract and Decentralized Application Platform. Abgerufen am 29.05.2019 von https://github.com/ethereum/wiki/wiki/White-Paper.

Buy Bitcoin Worldwide (Internetseite). Bitcoin Mining in China. Abgerufen am 29.05.2019 von https://www.buybitcoinworldwide.com/mining/china/.

Chohan, U. (2017). The Double Spending Problem and Cryptocurrencies. SSRN Electronic Journal. 10.2139/ssrn.3090174.

Cohen, R. (2013). Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined! Abgerufen am 29.05.2019 von https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/.

CoinMarketCap (Internetseite). All Cryptocurrencies. Abgerufen am 29.05.2019 von https://coinmarketcap.com/all/views/all/.

Delahaye, J.P. (2018). Bitcoin, der Energiefresser. Abgerufen am 29.05.2019 von https://www.spektrum.de/magazin/bitcoin-der-energiefresser/1547033.

Deloitte (Internetseite). Die Blockchain aus Sicht des Datenschutzrechts. Abgerufen am 29.05.2019 von https://www2.deloitte.com/dl/de/pages/legal/articles/blockchain-datenschutzrecht.html.

Deubel, M., Moormann, J., Holotiuk, F. (2017). Nutzung der Blockchain-Technologie in Geschäftsprozessen: Analyse am Beispiel des Zahlungsverkehrs. Abgerufen am 29.05.2019 von https://dl.gi.de/bitstream/handle/20.500.12116/4105/B10-5.pdf.

Digiconomist (Internetseite). Bitcoin Energy Consumption Index. Abgerufen am 29.05.2019 von https://digiconomist.net/bitcoin-energy-consumption.

Dölle, M. (2018). Ewiger Speicher – Die Blockchain als Datenmüllhalde. c't 2018 Heft 12, heise Verlag.

Dziembowski, S.; Faust, S.; Kolmogorov, V.; Pietrzak, K. (2015). Proofs of Space. Abgerufen am 29.05.2019 von https://www.ieee-security.org/TC/SP2014/posters/DZIEM.pdf.

E-Estonia (Internetseite). Security and Safety. Abgerufen am 29.05.2019 von https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/.

Einaste, T. (2018). Blockchain and healthcare: the Estonian experience. Abgerufen am 29.05.2019 von https://nortal.com/blog/blockchain-healthcare-estonia/.

Epple, S. (2018). Blockchain sticht in See: Digitalisierung von weltweiten Lieferketten. Abgerufen am 29.05.2019 von https://www.ibm.com/de-de/blogs/think/2018/01/25/blockchain-lieferketten/.

Erbguth, J. (2018). Datenschutz auf öffentlichen Blockchains. Abgerufen am 29.05.2019 von https://erbguth.ch/Erbguth_DatenschutzBlockchains.pdf.

Equibit Group (2017). Cryptocurrency Hash Functions - Equibit Group Chose SHA-3. Abgerufen am 29.05.2019 von https://www.equibitgroup.com/media-center-blog/cryptocurrency-hash-functions-equibit-group-chose-sha-3.

Fanusie, Y. J., Robinson T. (12.01.2018). Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services. Eine Studie der Foundation for Defense of Democracies kommt zu dem Schluss, dass weniger als 1 % der Bitcoin-Transaktionen auf illegale Aktivitäten hinweisen. Abgerufen am 29.05.2019 von http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.

Federal Information Processing Standards Publication (2002). FIPS PUB 180-2. Specifications for the Secure Hash Standard. Abgerufen am 29.05.2019 von https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2withchangenotice.pdf.

Fischer, M. (2017). Wegen Mining-Boom: Preise von AMD- und Nvidia-Grafikkarten steigen weiter. Abgerufen am 29.05.2019 von https://www.heise.de/newsticker/meldung/Wegen-Mining-Boom-Preise-von-AMD-und-Nvidia-Grafikkarten-steigen-weiter-3764812.html.

Flinterhoff, A. (2018). „Urheberrecht oder Eigentümerschaft mit der Blockchain digital absichern – für Kreative, Kunsteigentümer und Rechteinhaber". Abgerufen am 29.05.2019 von https://www.xing.com/communities/posts/urheberrecht-oder-eigentuemerschaft-mit-der-blockchain-digital-absichern-fuer-kreative-kunsteigentuemer-1014389687.

Förster, M. (2017). Hyperledger Fabric: IBM startet seine Blockchain as a Service. Abgerufen am 29.05.2019 von https://www.heise.de/newsticker/meldung/Hyperledger-Fabric-IBM-startet-seine-Blockchain-as-a-Service-3660165.html.

Github (Internetseite). Bitcoin: Quell-Code und Informationen. Abgerufen am 29.05.2019 von https://github.com/bitcoin/bitcoin.

Github (Internetseite). neo-project/neo – Network Protocol. Abgerufen am 29.05.2019 von https://github.com/neo-project/neo/wiki/Network-Protocol.

Github (Internetseite). Proof of Stake FAQ. Abgerufen am 29.05.2019 von https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.

Giese, P. (2018). Investment und 51-Prozent-Attacke: Der fundamentale Wert einer Kryptowährung. Abgerufen am 29.05.2019 von https://www.btc-echo.de/investment-und-51-prozent-attacke-der-fundamentale-wert-einer-kryptowaehrung/.

Giese, P. (2018). Token und Kryptowährungen – ein fundamentaler Unterschied. Abgerufen am 29.05.2019 von https://www.btc-echo.de/token-und-kryptowaehrungen-ein-fundamentaler-unterschied/.

Grech, A., Camilleri, A. F. (2017). Blockchain in Education. JRC Science for Policy Report. EU-Kommission. doi:10.2760/60649

Gruenderszene.de (2018). Nach Tod von Krypto-Investor: Hunderte Millionen Ripple verloren. Abgerufen am 29.05.2019 von https://www.gruenderszene.de/fintech/matthew-mellon-ripple-millionen-tod-verloren.

Hammersley, B. (2017). The most advanced digital society in the world is a former Soviet Republic on the edge of the Baltic Sea. Abgerufen am 29.05.2019 von http://www.wired.co.uk/article/estonia-e-resident.

Hongkong & Shanghai Banking Corporation Holdings PLC/HSBC (2017). Trust in Technology report. Abgerufen am 29.05.2019 von http://www.hsbc.com/news-and-insight/media-resources/media-releases/2017/~/media/hsbc-com/newsroomassets/2017/pdfs/170609-updated-trust-in-technology-final-report.pdf.

Hyperledger Sawtooth (Internetseite). Proof of Elapsed Time (PoET). Abgerufen am 29.05.2019 von https://sawtooth.hyperledger.org/docs/core/nightly/0-8/introduction.html.

Institute of Electrical and Electronics Engineers (Internetseite). IEEE 802.x Standards. Abgerufen am 29.05.2019 von https://ieeexplore.ieee.org/browse/standards/getprogram/page/series?id=68.

Kannenberg, A. (2014). Bitcoin: Erstmals gefährliche Konzentration der Mining-Leistung. Abgerufen am 29.05.2019 von https://www.heise.de/newsticker/meldung/Bitcoin-Erstmals-gefaehrliche-Konzentration-der-Mining-Leistung-2224113.html.

Kannenberg, A. (2018). Bösartiger Miner: 51-Prozent-Attacke und Double-Spend gegen Bitcoin Gold. Abgerufen am 29.05.2019 von https://www.heise.de/newsticker/meldung/Boesartiger-Miner-51-Prozent-Attacke-und-Double-Spend-gegen-Bitcoin-Gold-4058874.html.

Kharif, O. (2018). Bitcoin may split 50 times in 2018 as forking craze mounts. Abgerufen am 29.05.2019 von https://economictimes.indiatimes.com/markets/stocks/news/bitcoin-may-split-50-times-in-2018-as-forking-craze-mounts/articleshow/62628486.cms.

Kilic, K. (2018). So funktioniert das Lightning Network von Bitcoin. Abgerufen am 29.05.2019 von https://www.wired.de/collection/tech/so-funktioniert-das-lightning-network-fuer-bitcoin.

Krawczyk, H., Rabin, T. (2000). Chameleon Signatures. Abgerufen am 29.05.2019 von http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/Chameleon-Signatures-paper-Hugo-Krawczyk.pdf.

Lantmäteriet, Kairos Future, Telia Company, ChromaWay, SBAB, Landshypotek Bank (2017). The Land Registry in the blockchain – testbed. Abgerufen am 29.05.2019 von https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf.

Learn Cryptography (Internetseite). 51% attack. Abgerufen am 29.05.2019 von https://learncryptography.com/cryptocurrency/51-attack.

Learn Cryptography (Internetseite). Prime Factorization. Abgerufen am 29.05.2019 von https://learncryptography.com/mathematics/prime-factorization.

Lexas Länderdaten (Internetseite). Stromverbrauch im weltweiten Ländervergleich. Abgerufen am 29.05.2019 von https://www.laenderdaten.de/energiewirtschaft/elektrische_energie/stromverbrauch.aspx.

Louven, S. (2018). Santander will Blockchain-Technologie nutzen. Abgerufen am 29.05.2019 von http://app.handelsblatt.com/finanzen/banken/spanische-banken-santander-will-blockchain-technologie-nutzen/20910600.html.

Mathepedia (Internetseite). Injektive Abbildungen. Abgerufen am 29.05.2019 von http://www.mathepedia.de/Injektion.html.

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O. und Wehrle, K. (2018). Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. Abgerufen am 29.05.2019 von https://fc18.ifca.ai/preproceedings/6.pdf.

Medium.com, Song, J. (2018). Why Blockchain is Hard. Abgerufen am 29.05.2019 von https://medium.com/@jimmysong/why-blockchain-is-hard-60416ea4c5c.

Meier, S. (2017). Wie Blockchain den Arbeitsmarkt verändert. Abgerufen am 29.05.2019 von https://www.boersenblatt.net/bookbytes/artikel-wie_blockchain_den_arbeitsmarkt_veraendert.1355592.html.

Merkel, K. (2018). „Blockchain wird die Macht der Tech-Riesen schmälern". Abgerufen am 29.05.2019 von https://www.handelszeitung.ch/digital-switzerland/blockchain-wird-die-macht-der-tech-riesen-schmalern.

Merkle, R. C. (1979). Method of providing digital signatures. Leland Stanford Junior University: US4309569A.

MIT Laboratory for Computer Science and RSA Data Security, Rivest, R. (1992). The MD5 Message-Digest Algorithm. Abgerufen am 29.05.2019 von https://tools.ietf.org/html/rfc1321.

Moller, A. P. (2018). Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains. Abgerufen am 29.05.2019 von https://www-03.ibm.com/press/us/en/pressrelease/53602.wss.

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Abgerufen am 29.05.2019 von https://bitcoin.org/bitcoin.pdf.

National Institute of Standards and Technology (Internetseite). Cryptographic Standards and Guidelines. Abgerufen am 29.05.2019 von https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development.

Needham, R. M. und Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. Palo Alto: Xerox Palo Alto Research Center.

Nussbaum, J. (2017). Blockchain Project Ecosystem. Abgerufen am 29.05.2019 von https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940ababaf27.

Okupski, K. (2016). Bitcoin developer reference. Technische Universität Eindhoven. Abgerufen am 29.05.2019 von https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf.

Peck, M. E. (2017). Why the Biggest Bitcoin Mines Are in China. Abgerufen am 29.05.2019 von https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china.

Poon, J., Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Abgerufen am 29.05.2019 von https://lightning.network/lightning-network-paper.pdf.

Popov, S. (2018). The Tangle. Abgerufen am 29.05.2019 von https://iota.org/IOTA_Whitepaper.pdf.

Roßbach, P. (2016). Blockchain-Technologien und ihre Implikationen. Abgerufen am 29.05.2019 von http://blog.frankfurt-school.de/blockchain-technologien-konsens-mechanismen/?lang=de.

Ryte Wiki (Internetseite). Definition Dark Web. Abgerufen am 29.05.2019 von https://de.ryte.com/wiki/Dark_Web.

Schwartz, D., Youngs, N., Britto, A. (2014). The Ripple Protocol Consensus Algorithm. Abgerufen am 29.05.2019 von https://ripple.com/files/ripple_consensus_whitepaper.pdf.

Schwirzke, K. (2016). Blockchain-Technik: Musikwirtschaft sucht Auswege aus der Datenflut. Abgerufen am 29.05.2019 von https://www.heise.de/newsticker/meldung/Blockchain-Technik-Musikwirtschaft-sucht-Auswege-aus-der-Datenflut-3310684.html.

Sedgewick, R. und Wayne, K. (2014). Algorithmen und Datenstrukturen. München: Pearson Studium.

Sihvart, M. (2017). Blockchain – security control for government registers. Abgerufen am 29.05.2019 von https://e-estonia.com/blockchain-security-control-for-government-registers/.

Slimcoin (2014). Slimcoin: A Peer-to-Peer Crypto-Currency with Proof-of-Burn. Abgerufen am 29.05.2019 von https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf.

Soprasteria (2017). Potenzialanalyse Blockchain-Technologie. Abgerufen am 29.05.2019 von https://www.soprasteria.de/newsroom/publikationen/studie/potenzialanalyse-blockchain-technologie.

Spiegel.de (2018). Cambridge-Analytica-Skandal: Zahl der Geschädigten deutlich höher als bislang bekannt. Abgerufen am 29.05.2019 von http://www.spiegel.de/netzwelt/web/facebook-skandal-daten-von-87-millionen-nutzern-betroffen-a-1201288.html.

Swan, M. (2015). Blockchain: Blockchain: Blueprint for a new economy. UK: O'Reilly.

Tagesanzeiger (Internetseite). „Ob diese Technologie Jobs vernichtet? Massenweise!". Abgerufen am 29.05.2019 von https://www.tagesanzeiger.ch/wirtschaft/standardob-diese-technologie-jobs-vernichtet-massenweise-ja/story/24824106.

Tanenbaum, A. und van Steen, M. (2007). Verteilte Systeme: Prinzipien und Paradigmen. München: Pearson Studium.

The Economist (2015). The promise of the blockchain – The trust machine. Abgerufen am 29.05.2019 von https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Tuwiner, J. (2017). Bitcoin-Mining Hardware ASICs und Rigs. Abgerufen am 29.05.2019 von https://www.buybitcoinworldwide.com/de/mining-hardware-asics/.

Tuwiner, J. (2018). Bitcoin Mining in China. Abgerufen am 29.05.2019 von https://www.buybitcoinworldwide.com/mining/china/.

Uken, M. (2017). Kryptowährungen: „Deutschland ist Bitcoin-Diaspora". Abgerufen am 29.05.2019 von https://www.zeit.de/wirtschaft/geldanlage/2017-12/kryptowaehrungen-bitcoin-boerse-spekulation-oliver-flaskaemper/komplettansicht.

VDI Technologiezentrum (2018). Blockchain – eine Technologie mit disruptivem Charakter. Düsseldorf: VDI Technologiezentrum GmbH.

Voshmgir, S., Kalinov, V. (2017). Blockchain Handbook: A Beginners Guide. Abgerufen am 29.05.2019 von https://s3.eu-west-2.amazonaws.com/blockchainhub.media/Blockchain+Technology+Handbook.pdf.

Welzel, C., Eckert, K. P., Kirstein, F., Jacumeit, V. (2017). Mythos Blockchain: Herausforderung für den öffentlichen Sektor vom Kompetenzzentrum öffentliche Informationstechnologie. Abgerufen am 29.05.2019 von https://www.oeffentliche-it.de/documents/10181/14412/Mythos+Blockchain+-+Herausforderung+f%C3%BCr+den+%C3%96ffentlichen+Sektor.

Wikipedia (Internetseite). Decentralized Autonomous Organization (DAO). Abgerufen am 29.05.2019 von https://de.wikipedia.org/wiki/Ethereum#Decentralized_Autonomous_Organization_(DAO).

Wikipedia (Internetseite). Gig Economy. Abgerufen am 29.05.2019 von https://de.wikipedia.org/wiki/Gig_Economy.

Wikipedia (Internetseite). Napster. Abgerufen am 29.05.2019 von https://de.wikipedia.org/wiki/Napster.

Wikipedia (Internetseite). Vertrauen. Abgerufen am 29.05.2019 von https://de.wikipedia.org/wiki/Vertrauen.

Wikipedia (Internetseite). Zero-Knowledge-Beweis. Abgerufen am 29.05.2019 von https://de.wikipedia.org/wiki/Zero-Knowledge-Beweis.

Wyman, O. (2016). Blockchain in Capital Markets. Abgerufen am 29.05.2019 von http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/BlockChain-In-Capital-Markets.pdf.

YouGov (2017). Blockchain-Revolution. Abgerufen am 29.05.2019 von https://campaign.yougov.com/DE_2017_08_Reports_Blockchain_Landingpage.html.

Zamfir, V. (2017). Casper the Friendly Finality Gadget (FFG). Abgerufen am 29.05.2019 von https://github.com/ethereum/research/blob/master/papers/CasperTFG/CasperTFG.pdf.

Abbildungsverzeichnis

ABBILDUNG 1: Google-Suchanfragenverlauf zu populären IT-Themen 08

ABBILDUNG 2: Verteilte Architektur (links), zentralisierte Architektur (rechts) 10

ABBILDUNG 3: Hybridarchitektur 11

ABBILDUNG 4: Ein binärer Hash-Baum mit sukzessiv kombinierter Hash-Wurzel 19

ABBILDUNG 5: Symmetrische und asymmetrische Verschlüsselungsverfahren 22

ABBILDUNG 6: Funktionsweise einer digitalen Signatur zur Überprüfung einer Transaktion 24

ABBILDUNG 7: Schematischer Aufbau eines Blocks einer Blockchain 26

ABBILDUNG 8: Verkettung der Blöcke über den Block-Hash des Vorgängerblocks 27

ABBILDUNG 9: Zwei Transaktionen T3 und T4 sollen an eine Blockchain angehängt werden 28

ABBILDUNG 10: Die Hash-Wurzel H34 wird aus der Transaktionen T3 und T4 erstellt 29

ABBILDUNG 11: Blockheader 2 des neuen Blocks wird generiert 29

ABBILDUNG 12: B2 ist neuer Kopf der aktualisierten Blockchain 30

ABBILDUNG 13: Veränderungen in Blöcken führen zu inkonsistenten Hash-Werten 30

ABBILDUNG 14: Die verschiedenen Komponenten des Hash-Puzzles 33

ABBILDUNG 15: Entwicklung der Hash-Wert-Leistung des Bitcoin-Netzwerks 34

ABBILDUNG 16: Ansätze zur DSGVO-Compliance 43

ABBILDUNG 17: Marktanteil der größten Bitcoin Mining Pools 44

ABBILDUNG 18: Google-Suchanfragenverlauf zu populären IT-Themen 47

ABBILDUNG 19: Blockchain Project Ecosystem 52

ABBILDUNG 20: Public (Bitcoin-Adresse) und Private Key eines Bitcoin-Paper Wallets 55

ABBILDUNG 21: Architektur einer Blockcerts-Anwendung 61

ABBILDUNG 22: Vergleich von offenen und geschlossenen Blockchain-Architekturen 63

ABBILDUNG 23: Der Tangle von IOTA 69

ABBILDUNG 24: Unterscheidung und Beziehung von Szenario, Anwendungsfall und Implementierung von Blockchain-Technologie 77

ABBILDUNG 25: ENIC-NARIC-Ablaufplan für die Verifizierung von Bildungsnachweisen 83

ABBILDUNG 26: Ablauf für die Weitergabe und Verifizierung von erfahrungsbasierten Zertifikaten auf einer Blockchain 86

Tabellenverzeichnis

TABELLE 1: Mapping auf den Anfangsbuchstaben des Nachnamens 15

TABELLE 2: Abbildung verschieden langer Eingabewerte auf Ausgaben konstanter Länge 16

TABELLE 3: Auswirkungen von Veränderungen auf den berechneten Hash-Wert 17

TABELLE 4: Finden eines Nonce, der, angehängt an eine Nachricht, einen Hash-Wert mit z. B. fünf führenden Nullen erzeugt 20

TABELLE 5: Die Top 20 der marktkapitalstärksten Kryptowährungen 51

TABELLE 6: Stakeholder-Bewertung der Blockchain-Anwendungsfälle 103

Verzeichnis der Einsatzszenarien von Blockchain im Hochschulbildungsbereich

BILDUNGSNACHWEISE BEGLAUBIGEN, AUSSTELLEN UND ANERKENNEN (ABSCHNITT 4.3) 78
Ausstellung beglaubigter Bildungsnachweise (Abschnitt 4.3.5) 84
Verifizierung von Zertifikaten (Abschnitt 4.3.6) 84
Verifizierte digitale Identitäten für Hochschulen (Abschnitt 4.3.7) 84
Automatische Übertragung und Akkumulierung von Studienleistungen (Credits) (Abschnitt 4.3.8) 85
Teilen und Verifizieren von Nachweisen erfahrungsbasierter Kompetenzen (Abschnitt 4.3.9) 86

SOFTWARE UND DATEN IN LEHRE UND STUDIUM DEZENTRALISIEREN (ABSCHNITT 4.4) 88
Dezentralisierte Social Apps für den Bildungsbereich (Abschnitt 4.4.3) 90

STUDIERENDENDATEN IN DER VERWALTUNG MINIMIEREN (ABSCHNITT 4.5) 91
Management der Studierendenidentität im Hochschulbildungssystem (Abschnitt 4.5.4) 93

AKADEMISCHE INHALTE UND WERKE NACHVERFOLGEN (ABSCHNITT 4.6) 94
Beglaubigung von Autorenschaften und IP-Rechten (Abschnitt 4.6.4) 96
Nachverfolgung der Nutzung von akademischen Inhalten und Werken (Abschnitt 4.6.5) 96

ZAHLUNGEN UND MITTELFLÜSSE MANAGEN (ABSCHNITT 4.7) 97
Zahlung von Studiengebühren (Abschnitt 4.7.3) 99
Studienförderung (Abschnitt 4.7.4) 99
Leistungsbezogene Mittelzuweisung (Abschnitt 4.7.5) 99

WEITERE SZENARIEN (ABSCHNITT 4.8) 101
Wahlen (Abschnitt 4.8.1) 101
Dezentralisierte Autonome Organisationen (Abschnitt 4.8.2) 101
Integration in den gesamten Forschungsprozess (Abschnitt 4.8.3) 101
Prüfungen (Abschnitt 4.8.4) 102

Verschlagwortete Literatur

Zur Identifikation geeigneter Literatur und Quellen war für die Recherche der inhaltliche Fokus der Studie handlungsleitend. Die gesamte Recherche erfolgte nach dem „Schneeballprinzip". Ausgangspunkt waren aktuelle Studien mit Review-Charakter und hier wurde insbesondere auch die EU-Studie „Blockchain for Education: A study on the digital accreditation of personal and academic learning" von Grech und Camilleri mit fast 100 Referenzen als Grundlage berücksichtigt. Zur Identifikation weiterer Quellen wurden eine allgemeine Internetrecherche durchgeführt und Publikationen führender Think Tanks untersucht. Zusätzlich wurden auch populäre Weblogs wie „Bitcoin Magazine", „Blockchain Blog" sowie Twitter-Influencer und laufende Aktivitäten global agierender Blockchain Hubs ausgewertet. Berichte, insbesondere von Unternehmen, die sich einer der drei großen Blockchain-Allianzen „Hyperledger", „R3" und „Enterprise Ethereum Alliance" angeschlossen haben, wurden ebenfalls untersucht. Ergänzend erfolgte eine systematische Recherche mit Suchbegriff-Kombinationen, z. B. „blockchain" AND „proof-of" oder „blockchain" AND „education". Die Suchbegriffe wurden im Vorfeld systematisch kuratiert, um z. B. Synonyme, Homonyme, Singular-und Plural-Formen abzubilden. Die Zitate in den identifizierten Publikationen waren wiederum Startpunkt für eine neue Rechercherunde. Über den gesamten Zeitraum fand eine fortlaufende Aktualisierung der Literaturlisten & Referenzprojekte statt.

Initiativen im Bereich Blockchain in der Hochschulbildung

TYPEN

Prä-ICO
Derzeit ist dies eine Idee, die über ein ICO (Initial Coin Offering) Geld sammelt.

Post-ICO
Geld wurde online durch ein ICO (Initial Coin Offering) gesammelt und ein erstes Produkt wird entwickelt/eingeführt.

Code/Standard
Ein Code oder Standard wurde veröffentlicht, der diese Art der Anwendung ermöglicht.

Unternehmen
Die Initiative wird von einem privaten Unternehmen gefördert.

Andere
Andere Art von Initiative

INITIATIVE	TYP	SZENARIO / ANWENDUNG	URL	BESCHREIBUNG
GLEDOS*	Prä-ICO	Zahlungsmanagement Ausstellung von Zertifikaten	https://gledos.io	Gledos will ein Bildungsmarktplatz sein, der es den Studierenden ermöglicht, mithilfe von Mikro-Lernmodulen verschiedener Anbieter maßgeschneiderte Lernpfade aufzubauen. Blockchain wird verwendet, um die Zahlungen zwischen den Studenten und den vielen verschiedenen Lieferanten zu verwalten und die Leistungen zu dokumentieren.
ACCREDIBLE	Unternehmen	Beglaubigung von Zertifikaten	https://www.accredible.com/	Accredible bietet eine Kombination aus digitalen PDF-Zertifikaten und offenen Ausweisen. Sie erlaubt es den Kunden nun auch, diese Zertifikate auf der Bitcoin-Blockkette ohne zusätzliche Kosten zu beglaubigen. Zertifikate sind unabhängig überprüfbar.
MICROHE	Code	Ausstellung von Zertifikaten	https://microcredentials.eu/	MicroHE ist ein vom Erasmus+-Programm finanziertes Projekt, das einen Standard für die Speicherung und den Austausch von Bildungsnachweisen in der Blockchain basierend auf dem Ethereum ERC-721 Token veröffentlicht.
BLOCKCERTS	Code	Beglaubigung von Zertifikaten	https://www.blockcerts.org/guide/	Blockcerts ist eine offene Standard- und Open-Source-Codebasis für die Erstellung von Anwendungen, die blockkettenbasierte offizielle Datensätze ausgeben und verifizieren. Die meisten Akteure im Feld verwenden Blockcerts oder eine Fork davon für ihre Produkte.
EDUCTX	Code	Ausstellung von Zertifikaten	https://eductx.org/	Die EDUCTx-Lösung verarbeitet, verwaltet und steuert ECTX-Token verschiedener Typen und Transaktionen, basierend auf einem weltweit verteilten P2P-(Peer-To-Peer)Netzwerk aus Universitäten. Die Tokenisierung innerhalb der Plattform kann auf dem Konzept von ECTS basieren, wobei 1 Token einem ECTS-Punkt entspricht.
LEARNING MACHINE	Unternehmen	Beglaubigung von Zertifikaten	https://www.learningmachine.com/	Learning Machine bietet Software, die Zertifikate auf Basis von Blockcerts ausstellt und verifiziert. Es bietet keine öffentliche Middleware-Lösung, sondern arbeitet ausschließlich an einem Business-to-Business und Business-to-Government-Modell für große Implementierungen. Zertifikate sind unabhängig überprüfbar.
GRADBASE	Unternehmen	Beglaubigung von Zertifikaten	https://www.gradba.se	Gradbase bietet die Beglaubigung und Verifizierung von digitalen Zertifikaten auf einer Blockchain an. Das System ist vollständig geschlossen und proprietär.
WOOLF UNIVERSITY	Prä-ICO	Zahlungsmanagement Ausstellung von Zertifikaten	https://woolf.university/	Woolf University ist eine Initiative der Universität Oxford, die eine akkreditierte Universität gründen will, die Abschlüsse im Rahmen von Online-Tutorials anbietet. Woolf will mithilfe von Smart Contracts die gesamte Hochschulverwaltung automatisieren. Dazu gehören zunächst Zahlungen und Kreditübertragungen, Leistungsnachweise und Abstimmungen über Projekte und Budgets.

* Hinweis: Der Autor Anthony F. Camilleri berät diese Initiative.

INITIATIVE	TYP	SZENARIO/ ANWENDUNG	URL	BESCHREIBUNG
PKI CERTIFICATES	Code	Verwaltung von PKI Zertifikaten	https://github.com/snt-sedan/pki-blockchain	Ein Blockchain-basiertes PKI-Management-Framework zur Ausstellung, Validierung und Sperrung von X.509-Zertifikaten.
LEDGER JOURNAL	Andere	Verwaltung von geistigem Eigentum	http://ledgerjournal.org	Die Zeitschrift veröffentlicht Forschungen über die Blockchain und fordert die Benutzer auf, ihre Dokumente mit ihren privaten Bitcoin-Schlüsseln digital zu signieren, sowie Zeitstempel von veröffentlichten Manuskripten in der Blockchain. Zusätzlich hat das Journal Open-Source-Plug-ins für Open Journal Systems entwickelt, die es jedem, der die Software betreibt, ermöglichen, auch Zeitschriftenartikel auf der Blockchain zu signieren und mit einem Zeitstempel zu versehen.
BINDED	Unternehmen	Verwaltung von geistigem Eigentum	https://binded.com/	Binded (früher bekannt als BlockAI) ist ein Copyright-Registrierungsdienst für Bilder in der Blockchain. Wenn ein Bild erstellt wird, kann sein Autor das Bild in den Dienst hochladen, und ein Hash dieses Bildes, zusammen mit dem Zeitstempel, wann es hochgeladen wurde, und die Identität des Autors werden in einer Blockchain registriert.
BERNSTEIN	Unternehmen	Verwaltung von geistigem Eigentum	https://www.bernstein.io/	Bernstein Technologies registriert den Hash von Dokumenten in der Blockchain und liefert damit den Beweis für Existenz, Integrität und Eigentum. Sie ist spezialisiert auf das Geltendmachen von Ansprüchen an geistiges Eigentum, welches dann zur Sicherung von Urheberrechten oder Patenten verwendet werden kann.
EVERIPEDIA	Unternehmen	Verwaltung von geistigem Eigentum	https://everipedia.org/	Everipedia ist eine Fork von Wikipedia, die Benutzer in Form von IQ-Tokens für das Kuratieren und Einreichen von Inhalten in dessen Wiki belohnt. Die dezentrale Datenbank schafft ein anregendes Peer-to-Peer-Netzwerk für die Einreichung, Kuratierung und Verwaltung einer Datenbank mit Enzyklopädie-Artikeln. Es wird vollständig von IQ-Token-Inhabern verwaltet, die Bearbeitungen genehmigen, netzwerkweite Regeln für die Enzyklopädie erstellen sowie Dienste für Token im Netzwerk kaufen und verkaufen können.
BITDEGREE	Post-ICO	Zahlungsmanagement Dezentralisierte Apps Schutz vertraulicher Informationen von Studierenden	https://www.bitdegree.org/	BitDegree ist eine Online-Mikro-Lernplattform, die Kurse im MOOC-Stil anbietet. Es wird Sponsoren ermöglichen, Smart Contracts zur Bezahlung von Kursen zu erstellen, deren Gelder nach Abschluss bestimmter Lernziele und -ziele an die Studenten freigegeben werden. Die Plattform bietet eine Reihe wichtiger Dienste: Identitätsregister, Kursmaterial-Repository, Kursmaterialindex, Bewertungswerkzeuge, Sponsoringbereich, Studienbereich und Leistungsbetrachter.
GRAPHITE DOCS	Andere	Dezentralisierte Apps	https://www.graphitedocs.com	Graphite Docs nutzt das Blockstack-Netzwerk, um eine dezentral verschlüsselte Version einer Online-Office-Suite zu erstellen.
FRAUNHOFER BLOCKCHAIN FOR EDUCATION	Andere	Zertifizierung	https://www.fit.fraunhofer.de/de/fb/cscw/projects/blockchain-for-education.html	Das Fraunhofer-Institut entwickelt ein offenes Projekt für Blockchain-Zertifikate mit dem Ziel, die Identität von Akkreditierungsstellen, Zertifizierungsstellen und Emittenten in der Chain sowie die Hashes von Bildungszertifikaten zu speichern.

Checkliste für Anforderungen an den Einsatz von Blockchain

AKTEURE/TEILNEHMER	JA
Sind die Teilnehmer unbekannt oder von unbekannter Vertrauenswürdigkeit?	○
Misstrauen sich die Akteure gegenseitig (nicht nur Teilnehmer-Teilnehmer sondern auch Teilnehmer-Intermediäre, Intermediäre-Intermediäre)? Sind die Teilnehmer unbekannt oder von unbekannter Vertrauenswürdigkeit?	○
Ist die Abschaffung von Intermediären bzw. zentralen Kontrollinstanzen erwünscht?	○
Agiert eine unbekannte Anzahl von Teilnehmern schreibend im System?	○
Sind die Parteien/Akteure gleichwertig in ihrer Funktion & haben die gleichen Rechte?	○
Soll der Daten-/Informationseigentümer exklusiv über seine Daten bestimmen und die Verwaltungsverantwortung an den Eigentümer übergeben werden?	○
Können Transparenz, Vertraulichkeit und Datenschutz länderübergreifend sichergestellt werden?	○

AKTEURE/SYSTEM	JA
Können bestehende Architekturen/Systeme die Anforderungen des jeweiligen Szenarios konzeptionell nicht erfüllen (auch nicht über angepasste Regeln, Normen, Standards, Vereinbarungen oder technische Erweiterungen)?	○
Sind die bestehenden Architekturen des jeweiligen Szenarios besonders gefährdet („Single Point of Attack“ oder „Single Point of Failure“), sodass eine permanente Replikation des gesamten Systems auf viele Knoten in einem Netzwerk notwendig ist?	○
Ist eine (vollständige) Dezentralisierung in ein verteiltes System sinnvoll/erwünscht, d. h. eine klassische Client-Server-Architektur ist für das Szenario ungeeignet oder es überwiegen die Vorteile der P2P-Architektur („Gleiche unter Gleichen“)?	○
Ist keine laufende Kontrolle oder Regulierung des Systems nötig (Software, Quellcode, Betrieb/Wartung, Updates) und läuft das System weitgehend autonom und wartungsarm? Soll der administrative und regulierende Einfluss aufgegeben werden?	○
Können Grundprinzipien und Regeln umfassend genug formuliert werden, sodass künftig keine oder wenige nachträgliche Änderungen am System erforderlich sind?	○
Gibt es ein einheitliches Datenschema? Sind diese Daten normiert?	○
Soll das System, einmal eingeführt, auf unbestimmte Zeit laufen, ohne dass die Informationen parallel konventionell weiter verwaltet werden müssen?	○
Können Grundprinzipien und Regeln umfassend genug formuliert werden, sodass künftig keine oder wenige nachträgliche Änderungen am System erforderlich sind?	○
Kann/Soll gewährleistet werden, dass das angestrebte System auch künftig (+20 Jahre) die Anforderungen erfüllt (z. B. Sicherheit, Skalierbarkeit, Zuverlässigkeit, Selbstsouveränität, gesetzliche Rahmenbedingungen)?	○

IMPRESSUM

Bibliografische Information der Deutschen Nationalbibliothek. Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN: 987-3-922275-91-6

Verwaltungsgesellschaft für Wissenschaftspflege mbH,
Essen 2019
Barkhovenallee 1
45239 Essen
T 0201 8401-181
F 0201 8401-459

Stand: 6. September 2018 | Literatur berücksichtigt bis einschließlich 25. Mai 2018
Korrigierte Fassung vom 3. Juni 2019

Studie im Auftrag des Bundesministeriums für Bildung und Forschung

AUTOREN
Anthony F. Camilleri, Thomas Werner, Andreas Hoffknecht, Andreas Sorge

UNTER MITWIRKUNG VON
Isabel Schünemann, Florian Rampelt, Ronny Röwert, Florian Hanke, Helena Häußler, Gino Krüger, Mike Raschke

REDAKTION
Simone Höfer

FOTOS
istockphoto.com: nd3000, Kosamtu.

GRAFIK UND LAYOUT
TAU GmbH, Berlin

DRUCK
Druckerei Schmidt, Lünen

Wir danken folgenden Sachverständigen, die ihre Expertise in die Stakeholder-Diskussionen und Experteninterviews zu diesem Bericht eingebracht haben:

Joshua Broggi, Ilona Buchem, Perrine de Coetlogon, Axel Dürkop, Alex Grech, Lambert Heller, Raimund Matros, Martin Lee, Theo Mensen, Mario Oettler, Marloes Pomp, Hans Pongratz, Wolfgang Radenbach, Rene Rahrt, Natalie Smolenski, Johan Tillema, Anja Wagner, Andreas Wittke

Print kompensiert
ID-Nr. 1326493
www.bvdm-online.de

FSC www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C006990

STIFTERVERBAND
für die Deutsche Wissenschaft e.V.

Barkhovenallee 1
45239 Essen
T 0201 8401-0
F 0201 8401-301

www.stifterverband.org