Decentralized Web

Das Internet der Zukunft?

Benedikt Weber
benedikt.weber@mni.thm.de

Abbildung 1. Beispielhaftes Konzept eines dezentralen Netzwerks [shi18]

Abstract

The following paper deals with the question if the technology of a decentralized web could possibly be used in the future while replacing the currently well-established client-server architecture.

To discuss this question properly a wide range of knowledge over the current situation and the functionality of a decentralized web is necessary.

The paper starts with the explanation, why the term Web3 is used over the counterpart Web 3.0, which is because Web 3.0 references more the concept of a semantic web, while Web3 is mostly used while talking about the use case of blockchain in a new era of the internet.

It continues by giving insights on how the client-server architecture works and how the technology evolved over time to it's current state.

Also the major problems this architecture involves are extensively described, because these are the main reasons why a development towards a decentralized web is strongly needed. This includes (1) huge privacy issues regarding tech giants like GAFA [1] stockpiling customer data (2) the need of web services or platforms which act as intermediaries. Not only trusting them is a huge issue, these servers are more likely to be attacked which sometimes ends in downtimes or even data thefts.

[1] **G**oogle, **A**pple, **F**acebook und **A**mazon

These problems could be solved by peer-to-peer networks and the use of blockchain. This massively increasing technology enables clients to not only use web services but provide them to others simultaneously. In this case the omission of intermediate platforms holds huge advantages, amongst others (1) security improvements, because there is no such thing like one server that could be attacked (2) control over private data, because everyone is in the position to delete his data whenever he wants.

The problem with this technology lies in the implementation, because bugs which are not located beforehand can end in huge problems.

Therefore it is still a long way to a decentralized web, but there are already many organizations and companies working on it to improve every single aspect, in order to fulfill a transition to a free and safe web as it was intended to by it's founder.

1 Einleitung

Seitdem das Internet für die Öffentlichkeit freigegeben wurde, hat es sich in kurzer Zeit sehr stark entwickelt. Zu Beginn wurden immer mehr Computer miteinander verbunden, was den Datenaustausch massiv beschleunigte. Durch die Einführung der Standards von Tim Berners-Lee um 1990 [Kra08] wurde es relativ einfach, Webseiten mit wenigen Zeilen Code darzustellen. Dies ermöglichte es den Nutzern, schnell auf Informationen und Ressourcen zuzugreifen, die Navigation erfolgte dabei im Web durch Hyperlinks und Suchmaschinen. Diese Phase reicht bis ins Jahr 2003 und wird als Web 1.0 bezeichnet. Als Killer-Applikation [2] gilt der Web-Browser, der den Menschen Zugang zum World Wide Web gewährte. Mit der Einführung von Social-Media- und e-Commerce-Plattformen brach die Phase des sogenannten Web 2.0 an, in der wir uns derzeit befinden. Diese Phase wird als Frontend-Revolution bezeichnet [Vos19, S. 23]. Der bedeutendste Unterschied liegt dabei in der Zugriffsart: Während das Web 1.0 den Nutzern überwiegend lesenden Zugriff auf Ressourcen bot, konnten die Nutzer am Web 2.0 partizipieren und soziale Interaktionen durchführen. Im Web 1.0 gab es also Webseiten eines Betreibers, die sich Nutzer ansehen konnten. Im Web 2.0 standen dann Seiten wie Wikipedia zur Verfügung, deren Inhalt verschiedenste Seitenbesucher bearbeiten konnten. Für solchen Interaktionen wird jedoch immer ein Mittelsmann benötigt, also eine Plattform, die zwei Personen, die sich nicht kennen und nicht vertrauen, eine Möglichkeit des Austauschs bietet. Die dahinterliegende Infrastruktur nennt sich Client-Server-Architektur: Ein Server stellt einen Dienst zur Verfügung, auf den mehrere Clients Zugriff erhalten und sich somit untereinander verknüpfen können.

Doch obwohl es immer mehr Endgeräte mit Zugang zum Web gibt [Cis11], hat sich diese Struktur nicht verändert. Das Problem an dieser Stelle: Es entstehen Abhängigkeiten von den einzelnen Servern, die mittlerweile eine Vielzahl von Clients bedienen müssen, und die einen SPoF [3] darstellen. Und diese technischen Aspekte sind nicht einmal die größten Probleme, die das World Wide Web heute mit sich bringt. Denn Abhängigkeiten bestehen auch zwischen den Nutzern und den Anbietern der Web-Dienste, wodurch bei großen Nutzerzahlen enormer Einfluss auf die Gesellschaft ausgeübt werden kann. Des Weiteren verdrängen oft Tech-Giganten wie Google, Apple, Facebook oder Amazon [BSZ16] die Konkurrenz vom Markt, wodurch Nutzern oft keine richtigen Optionen bei der Auswahl der Dienste bleibt, denen sie ihre Daten anvertrauen. Dabei haben laut einer Umfrage Ende 2017 in Deutschland lediglich 32% der Befragten Vertrauen bezüglich der Einhaltung des Datenschutzes in Google, bei Facebook sind es gerade einmal 18% [Hor17]. Kommuniziert ein Client mit einem Server, speichert dieser Informationen über den Client, und der Nutzer gibt mit jedem Request einen Teil der Kontrolle über seine Privatsphäre preis [Vos19, S. 21].

Aus dieser Kritik heraus entstand die Idee des Decentralized Web, auch Web3 genannt. Beim Konzept der Dezentralisierung wird die Architektur von Clients und Servern aufgebrochen, denn das Netzwerk wird von „alle[n] Nutzer[n] und ein[em] Netzwerk unabhängiger Rechner und Server“ [Bon19] betrieben. Im Web3 verändert sich das Frontend, also die Seiten, wie sie heute existieren, nicht. Stattdessen verändert sich das Backend massiv, da andere grundlegende Technologien benötigt werden.

Das Ziel dieser Seminararbeit soll sein, dem Leser oder der Leserin einen einfachen und verständlichen Einblick in das Thema der Dezentralisierung zu gewähren, da das Web seine Geschichte des schnellen Wandels fortführen wird. Dabei stellt das Decentralized Web als solches eine Möglichkeit der Weiterentwicklung des

[2] Eine Anwendung, die einer bestimmten Technik zum Durchbruch verhalf [Dud19]

[3] Single Point of Failure: Die Komponente eines Systems, ohne die das System nicht betriebsbereit ist [ITW17]

heutigen Internets dar. Des Weiteren ist es wichtig, den Nutzern des Internets die Dringlichkeit der aktuellen Datenschutz-Problematik näher zu bringen, und gleichzeitig Lösungen für diese Probleme zu erörtern. Denn der strikte Rückzug aus personalisierten Webdiensten entspricht nicht dem Ziel des Internets und ist genauso wenig eine Lösung, wie die gesamten eigenen Daten ohne jegliche Kontrolle weiterzugeben, um irgendwann beispielsweise als gläserner Mensch dazustehen. Die Leser dieser Arbeit sollen genug Informationen an die Hand bekommen, um sich kritisch mit der aktuellen Situation des Internets auseinandersetzen zu können und gleichzeitig eine Einführung in eine Technik erhalten, die vielleicht in Zukunft Einzug in den Alltag halten wird.

2 Begriffsabgrenzung

Vor dem tieferen Einstieg in die Materie werden an dieser Stelle zuerst die wichtigen Begrifflichkeiten geklärt, die zum Verständnis der folgenden Ausarbeitung nötig sind.

Es geht dabei um die Begriffe Web1, Web2 und Web3 im Gegensatz zu Web 1.0, Web 2.0 und Web 3.0. Während den Begriffen Web1 und Web 1.0 beziehungsweise Web2 und Web 2.0 dieselbe Bedeutung zukommt, gibt es bei Web3 und Web 3.0 signifikante Unterschiede. Denn der Begriff Web 3.0 wird in den meisten Fällen mit dem *semantischen Web* in Verbindung gesetzt. Dieses Konzept wurde, wie das WWW selbst, von Tim Berners-Lee bereits 1994 ins Leben gerufen und im Jahr 2001 in einem Artikel veröffentlicht (Vgl. [Swe16]). Diese Art des Internets beschreibt dabei die Erweiterung des Web 2.0 dahingehend, den Daten im Web eine Bedeutung zu verleihen und diese Bedeutung Maschinen durch Metadaten zugänglich zu machen. Das Ziel ist ein "klügeresÏnternet, dass die Fragen von Nutzern auf menschlicher Ebene beantworten kann. Suchmaschinen im semantischen Web sollen beispielsweise unterscheiden können, ob ein Nutzer gerade ein Geldinstitut oder eine Parkbank sucht, wenn der Begriff "Bankëingegeben wird (Vgl. [Hil]). Für einen Einstieg in diesen Themenbereich wird die von Kate Ray im Jahr 2010 veröffentlichte Dokumentation [4] empfohlen, in der unter anderem Herr Berners-Lee interviewt wird. Diese Arbeit soll sich jedoch nicht um die Thematik des Verknüpfens von Daten handeln, sondern beschäftigt sich mit dem Einsatz von Dezentralisierung und Blockchain in der nächsten Generation des Webs. Um diesen Unterschied zu signalisieren, wird der Term Web3 konsistent verwendet, wie es auch Frau Voshmgir im Buch Token Economy zu ebenjenem Thema praktiziert. Eine Suche nach dem Term “web3“ liefert zusätzlich die Library `web3.js` zurück, die eine Anbindung an ein Ethereum Node, also eine Instanz eines Ethereum-Blockchain-Netzes bietet (Vgl. [Eth19a]). Auch die sogenannte Web3 Foundation (Vgl. [Web19a]) beschäftigt sich mit dem Einsatz von Blockchain in der nächsten Generation des Internets, und bei den Web3 Summits geht es ebenso um Dezentralisierung (Vgl. [Web19b]). Die Schreibweisen Web1 und Web2 sind weniger bekannt als Web 1.0 und Web 2.0, und werden aus diesem Grund nicht verwendet.

[4] https://vimeo.com/11529540

3 Das Web 2.0

Um überhaupt die Gründe für eine Weiterentwicklung des Internets in die dezentrale Richtung erläutern und diskutieren zu können, benötigt der Leser oder die Leserin tiefer gehende Informationen über die sowohl technische als auch gesellschaftliche Entwicklung und eine Darstellung der aktuellen Situation, die in den folgenden Kapiteln ausführlicher behandelt werden.

3.1 Unterschiede zum Web 1.0

Den genauen Anfang des Internets zu datieren ist kaum möglich, da es bis zur heutigen Verwendung viele Entwicklungen und Meilensteine gegeben hat, die alle in einer eigenen Ausarbeitung Platz finden würden. Um nur ein paar Eckdaten zu nennen: Nachdem die Sowjetunion 1957 den ersten Satellit “Sputnik“ ins All geschossen hat, wurden vor allem in den USA viele Forschungsprojekte vorangetrieben, unter anderem das von der ***A**dvanced **R**esearch **P**rojects **A**gency* ins Leben gerufene ARPANET. Dieses Netz verknüpfte zunächst vier Computer in verschiedenen amerikanischen Städten und ermöglichte dadurch den Informationsaustausch [Kra08]. Nach der Umstellung auf das vom amerikanischen Verteidigungsministeriums entwickelte Protokoll *TCP/IP* im Jahr 1983 [Hel02] stellte es die technische Grundlage für das Internet dar. Als weitaus wichtiger ist jedoch das Jahr 1991 zu betrachten, genauer den 6. August diesen Jahres. An dem Tag veröffentlichte Tim Berners-Lee

seine Vision des WWW, des World Wide Web, an der er zuvor am CERN [5] in der Schweiz gearbeitet hat [Fie16].

Bis zu diesem Tag interessierte er sich bereits für Hypertext und Verlinkungen, die über den lokalen Rechner hinausgehen, doch er findet kaum Gehör am konservativen und physik-lastigen CERN [Fie16]. Seine Veröffentlichung in Form der ersten Webseite der Welt schlägt dennoch ein, und er erhält Rückmeldungen aus aller Welt. Mit der Verbreitung und dem massentauglichen Einsatz von Computern und Browsern, die auf den grundlegenden Protokollen und Prinzipien von Tim basierten, begann die Phase, die später als Web 1.0 referenziert werden soll. Abstrahiert bot das Web in dieser Phase lesenden Zugriff: Durch graphische Oberflächen und das Erstellen von Webseiten ohne Kommandozeilen oder tiefgreifendes technisches Wissen konnten Informationen ins Netz gestellt und durch Hyperlinks miteinander verknüpft werden, auf die eine große Masse von Nutzern Zugriff hatten. Als Killer-Applikation dieser Phase gilt der Browser, durch den der Zugriff auf die Seiten ohne technische Hürden und graphisch anschaulich ermöglicht wurde. Dabei kamen Webserver zum Einsatz, die als eine Art Speicherort für die Webseiten dienten und diese unter einer spezifischen Adresse für andere Internet-Nutzer zugänglich machten [6]. Auch dieser Server wurde von Tim in seiner Zeit am CERN entwickelt. Und obwohl die 2. Phase des Webs viel veränderte und die Techniken weiterentwickelt wurden, blieb dieses grundlegende Konzept bestehen.

3.2 Technischer Aufbau des Webs

Mit der Zeit wurde das Internet und das WWW immer komplexer, und die technischen Strukturen mit ihnen. Es gibt immer mehr Geräte, die an das Internet angebunden sind und daran partizipieren, ebenso wie Anbieter von Webseiten und -diensten. Durch die schiere Masse an Geräten und Kommunikation wurden immer mehr Bereiche vernetzt und riesige Rechenzentren errichtet, um mit den derzeitigen Größenordnungen mithalten zu können. Das Konzept hinter der Technik jedoch ist relativ simpel und wird Client-Server-Architektur genannt. Clients, also die Geräte der Endnutzer, greifen auf Server zu, und damit auf Webseiten oder -dienste der jeweiligen Anbieter, die von den Servern bereitgestellt werden. Die Kommunikation zwischen Client und Server wird dabei über HTTP realisiert, ein Protokoll, das ebenfalls von Tim Berners-Lee Anfang der 1990er Jahre entwickelt wurde. Die Abkürzung steht für *Hyper Text Transfer Protokoll* und beinhaltet grundlegende Regeln, wie die Kommunikation zwischen Netzwerkgeräten vonstatten geht.

Im Regelfall schickt ein Client zuallererst eine Anfrage an den Server, um herauszufinden, ob dieser überhaupt bereit ist. Ist dies der Fall, antwortet der Server mit einer Erfolgs-Antwort, und der Client kann die benötigte Anfrage stellen. Wenn der Server die Bearbeitung fertig gestellt hat, sendet er eine Antwort an den Client, der diese zum Beispiel weiterverarbeiten kann (siehe Figure 2). An dieser Stelle ein Alltagsbeispiel, das wohl jeder Internetnutzer kennt: Eine Google-Suchanfrage. Navigiert ein Benutzer beispielsweise auf www.google.de, um eine Google-Suche durchzuführen, wird auf dem Gerät des Nutzers (dem Client) zuerst die Webseite mit der Suchleiste von Google geöffnet. Gibt der Nutzer nun "Wie wird das Wetter heuteïn die Suchleiste ein und betätigt die Suchen-Schaltfläche, wird eine HTTP-Anfrage an den Server von Google gesendet. Ist dieser erreichbar und bereit (was wohl die meiste Zeit der Fall sein dürfte), wird der Such-Term in der HTTP-Anfrage versendet. Der Server verwendet nun die Rechenleistung eines Rechenzentrums, um die benötigten Antwortdaten zu "berechnen". Dafür benötigt er Metadaten wie beispielsweise den Standort des Clients, der ebenfalls in der HTTP-Anfrage mitgesendet werden kann. Nachdem der Server die Wetterdaten für den jeweiligen Standort abgerufen hat, sendet er eine Antwort, ebenfalls mittels HTTP-Protokoll. Der Client, der auf diese Antwort gewartet hat, kann die Informationen nun graphisch aufbereiten und auf dem Display des Nutzers darstellen. Dieses Konzept ist zwar in den Jahren entsprechend der Gerätezahl und der HTTP-Kommunikation mit skaliert, stößt jedoch in einigen Punkten an seine Grenzen. An manchen Stellen birgt es sogar große Probleme. Und wenn man sich mit der Kritik am Web 2.0 befasst, sind technische Gegebenheiten nicht immer das Problem, in vielen Fällen aber die Ursache, weshalb die Rufe nach Dezentralisierung lauter werden. Aufgrund dessen spielt das Verständnis der dem Internet zugrunde liegenden Technik mindestens aus konzeptioneller Sicht eine nicht unerhebliche Rolle.

[5] Die Europäische Organisation für Kernforschung (Conseil Européen pour la Recherche Nucléaire) [Wel19]. Als Physiker und Informatiker arbeitete Berners-Lee an der Möglichkeit des Informationsaustauschs zwischen Wissenschaftlern und Institutionen auf der ganzen Welt [CER20].

[6] Die erste Website von Tim ist aus historischem Interesse noch immer unter http://info.cern.ch/hypertext/WWW/TheProject.html erreichbar

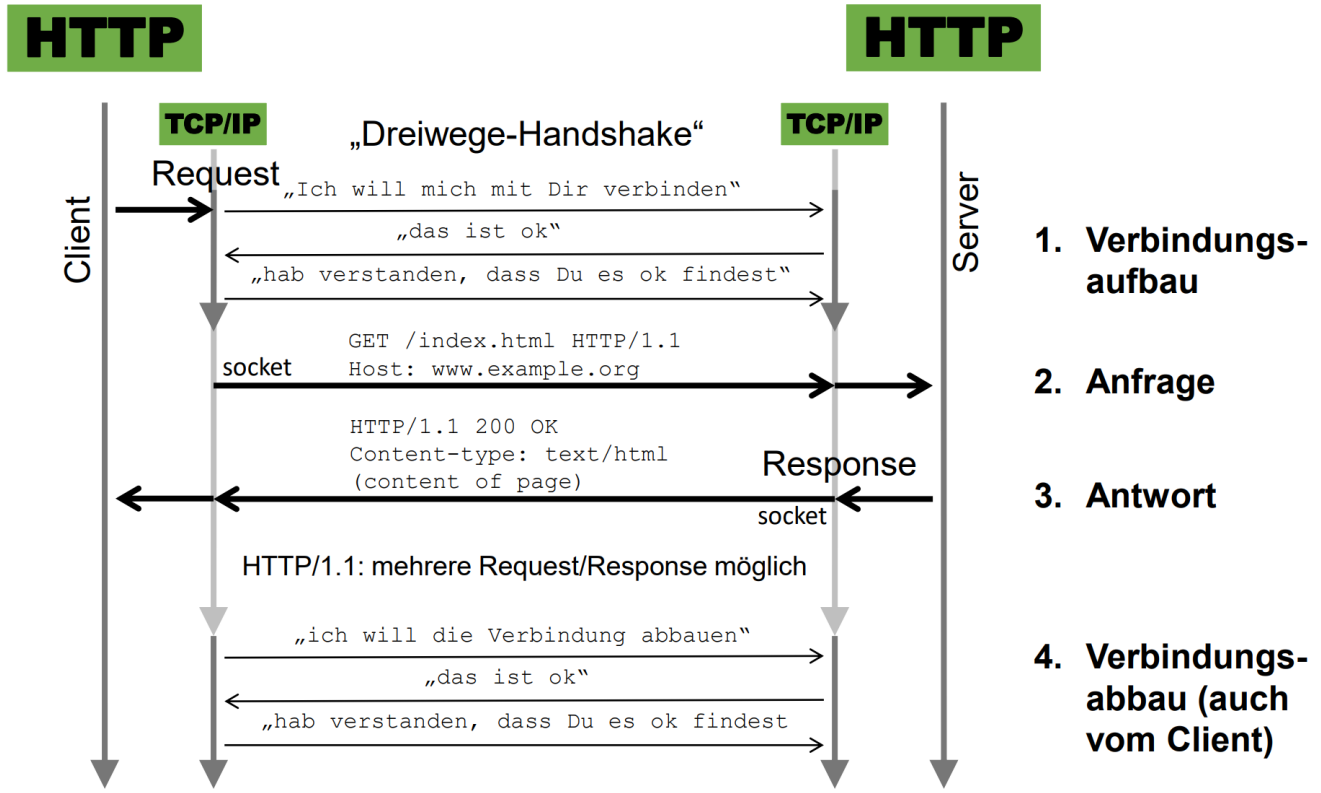

Abbildung 2. 3-Wege-Handshake bei einem HTTP-Request [KPR17]

3.3 Kritik und Problematik

Doch nun zu den Gründen, warum es überhaupt Menschen gibt, die sich mit dem Einsatz von neuen Techniken in der nächsten Generation des Internets beschäftigen. Wie bereits erwähnt hat sich das Internet schnell sehr stark entwickelt, um nicht zu sagen verändert. Dennoch basiert das grundlegende technische Konzept auf den Anfang der neunziger Jahre erfundenen Webservern. Doch wieso ist das schlecht, es funktioniert doch alles, oder? Diese Aussage ist theoretisch richtig, doch durch diese Struktur entstehen Probleme, die nicht auf den ersten Blick sichtbar sind und die viel zu lange inkonsequent behandelt wurden. Um das gewichtigste Problem an den Anfang zu stellen: Die Kontrolle über die eigenen Daten. Durch die im vorhergehenden Kapitel beschriebenen Plattformen, die als "Mittelsmann"dienen, ist es den Nutzern nahezu unmöglich, Einfluss auf die Speicherung und Verarbeitung der eigenen Daten zu nehmen. Die einzige Möglichkeit ist in den meisten Fällen, auf die Nutzung dieser Dienste oder sogar des gesamten Internets zu verzichten, was in der heutigen Zeit kaum möglich und auch nicht im Sinne des Erfinders ist. Zudem hat sich die Nutzung von Internet-Plattformen herauskristallisiert, hinter denen riesige Tech-Konzerne stehen, die international agieren und sich geschickt in der Umgehung von lokalen Gesetzen und Auflagen anstellen. Informationen über die Datenverarbeitung sind oft intransparent in seitenlangen Impressen versteckt, sodass diese einfach überlesen werden. Und selbst wenn man sich die Mühe des Entschlüsselns macht, hat man in der Regel keine Wahl: Man vertraut der Plattform mit der Nutzung die eigenen Daten an, oder eben nicht.

Das Unternehmen muss dabei nicht einmal selbst die Daten verkaufen, vermutlich ist dies ziemlich selten der Fall. Dennoch gibt es Andere, die das tun: Meldungen zu Datenschutzskandale in Form von geleakten oder gehackten Daten häufen sich. Zum Teil kursieren Datensätze mit Millionen von Nutzerdaten frei verkäuflich im Internet!

Dies kann nur geschehen, wenn die Systeme der Anbieter nicht ausreichend geschützt sind. Doch Hacker werden immer kreativer, und vor allem für kleinere Plattformen ist es schwierig, die Schutzmechanismen

auf dem neuesten Stand zu halten. Ein Grund für den Erfolg solcher Datendiebstähle ist, dass die Server in der beschriebenen CS-Struktur sogenannte SPOF's darstellen. Dies steht für *Single Point of Failure* und beschreibt in einem Hardware-System eine Komponente, ohne die das gesamte System nicht Betriebsbereit ist. Das Internet fällt zwar nicht aus, weil eine einzige Webseite offline ist, dennoch kann der Ausfall von verschiedenen Diensten und Plattform verheerende Folgen haben. Diese Ausfälle können sowohl durch Cyber- (oder sogar physischen) Angriffen als auch technischen Defekten entstehen. Diese können in beiden Fällen aufwendig zu Beheben sein und dadurch stundenlange Ausfälle verursachen. Bei Social-Media-Plattformen mag das keine verheerenden Auswirkungen haben, doch es gibt mittlerweile viele kritische Systeme, die ans Internet angeschlossen sind, und von denen zum Teil Leben abhängen.

Recap Abschließend die größten Probleme des Web 2.0 und damit die Gründe für ein dezentrales Internet zusammengefasst:

- Server stellen SPOF's dar, Ausfälle oder Attacken können verheerende Folgen haben
- Cyber-Attacken können in Datendiebstählen resultieren, Datensätze werden im Darknet an den meistbietenden verkauft
- Der gewöhnliche Verbraucher hat keine Einsicht in die eigenen Daten, geschweige denn die Kontrolle darüber

4 Das Web3

Dieses Kapitel beschäftigt sich nun mit Lösungsansätzen, die die zuvor genannten Probleme mit einer differenzierten Architektur lösen können. Dazu werden einige Beispiele für die Weiterentwicklung des Web 2.0 analysiert und das Web3 am Ende bewertet. Zuvor werden jedoch alle Leser und Leserinnen auf den gleichen Wissensstand gebracht, um den folgenden Ausführungen folgen zu können.

4.1 Grundlagen und Begrifflichkeiten

4.1.1 Dezentralisierung

Möchte man nun die zuvor analysierten Probleme des Web 1.0 beziehungsweise Web 2.0 umgehen, muss das Internet von der jetzigen Client-Server-Architektur zu einem dezentralen Aufbau wechseln. Das Ausmaß entspricht ungefähr dem von der Entwicklung des Web 1.0

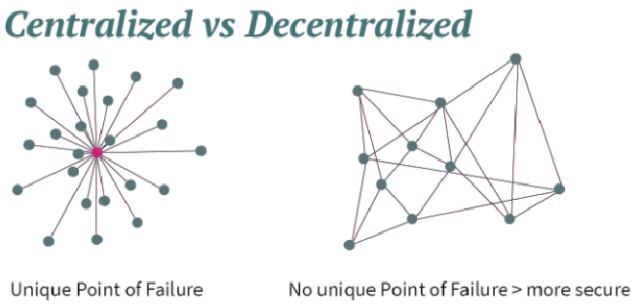

Abbildung 3. Unterschied zwischen zentraler und dezentraler Architektur [Blo19b]

.

zum Web 2.0. Während man jedoch bei dieser Entwicklung von einer Frontend-Revolution spricht, wird die Umstellung zum dezentralen Web eine Backend-Revolution werden. Der Unterschied? Wie in Kapitel 3 erläutert, charakterisiert das Web 2.0 unter anderem intuitive und nutzerfreundliche Webseiten bis hin zu Webapps. Da diese Seiten für die Nutzer sichtbar sind und sich im Vergleich zu den im Zeitalter des Web 1.0 vorhandenen puren HTML-Seiten radikal weiterentwickelt haben, spricht man von einer Frontend-Revolution. Die Art der Webseiten und -apps in einem dezentralen Internet werden sich jedoch zunächst einmal nicht maßgeblich verändern, sondern nur die zugrunde liegende Technik. Daher ist diese Entwicklung im Backend-Bereich angesiedelt und für den Anwender nicht direkt sichtbar.

Doch wie funktioniert die Dezentralisierung nun eigentlich? Im vorherigen Kapitel über das Web 2.0 wurde erläutert, dass Client-Server-Architekturen einen SPOF darstellen. In Abbildung 3 wird dieser SPOF als *Unique Point of Failure* dargestellt, dem die selbe Bedeutung zukommt. Aus der Abbildung wird der größte Unterschied sehr schnell ersichtlich: In einem dezentralen Netz gibt es keinen Server, auf den alle Clients zugreifen. Stattdessen kann jeder Computer Client und Server gleichzeitig sein. Fällt in diesem Szenario ein Gerät im Netzwerk aus, können die anderen Clients noch immer auf viele andere Computer im Netz zugreifen und so alle Dienste wie gewohnt weiterverwenden.

4.1.2 P2P-Netzwerk

P2P steht für Peer-to-Peer und bildet im Netzwerk-Kontext das grundlegende Konzept der Dezentralisierung. In einem Peer-to-Peer-Netzwerk sind alle Teilnehmer untereinander gleichberechtigt, wobei jeder Rechner Funktionen, Ressourcen oder Services anbieten oder

in Anspruch nehmen kann. Ein *Peer* kann dabei ein einzelner Rechner oder eine Gruppe von Rechnern sein. Ein P2P-Netz kommt ohne Server aus und ist demnach das Gegenteil einer Client-Server-Architektur [LD18].

4.1.3 Die Blockchain

Eine wichtige Technologie hin zum dezentralen Web ist Blockchain. Durch die von Satoshi Nakamoto [7] erfundene Kryptowährung wurde erstmals die Funktion der Währung und damit einhergehend auch der Blockchain erläutert. Die Blockchain selbst ist eine auf alle Netzwerkgeräte verteilte Datenbank, die sogenannte Blöcke mit Transaktionen enthält [CNP+16, S. 8]. Diese Transaktionen entstehen zwischen zwei Vertragspartnern und können von jedem Netzwerkteilnehmer verifiziert werden. Für diese Verifizierung wird Rechenleistung benötigt, die von sogenannten Minern für eine bestimmte Vergütung zur Verfügung gestellt wird. Nach der Verifizierung wird die Transaktion in einen Block der Blockchain geschrieben und im Netzwerk distribuiert. Eine Änderung ist ab diesem Punkt nicht mehr möglich, was diese Technik sicher vor Manipulationen und der Abhängigkeit von Vermittlungsplattformen (Intermediären) macht. Wird ein neuer Block hinzugefügt, verweist dieser auf den Hash-Wert des vorherigen Blocks, daher kommt auch der Name **Blockchain** (zu deutsch: Kette aus Blöcken).

Wie kann jedoch die Sicherheit der Transaktionen garantiert werden? Nun, der Quellcode der Blockchain ist Open Source und daher von allen Nutzern einsehbar. Und darin ist festgelegt, wie mit der Manipulation von einzelnen Transaktionen verfahren wird. Da die verifizierten Blöcke allen Netzwerkgeräten zur Verfügung gestellt werden und somit die "korrekte"Blockchain bekannt ist, werden Änderungen an dieser sofort erkannt und die entsprechenden Geräte aus dem Netzwerk ausgeschlossen. Für eine erfolgreiche Manipulation müssten demnach alle Blockchains auf allen Geräten verändert werden, was schier unmöglich ist.

4.1.4 Wallet

Um nun an einem Blockchain-Netzwerk teilhaben zu können, benötigt man ein sogenanntes Wallet. Dies ist eine Software, die bestimmte Algorithmen enthält und auf dem eigenen Client-Gerät ausgeführt wird. Um nun an den Vorgängen im Netzwerk teilhaben zu können, werden 2 Keys benötigt: Der Private und der Public Key. Der im ersten Schritt generierte Private Key ist ein zufällig-generierter 256-bit Integer, und sollte nicht weitergegeben werden. Er dient dazu, eigene Transaktionen zu signieren. Aus dem Private Key wird im zweiten Schritt mittels *Elliptic-Curve- Cryptography* der Public Key generiert. Diese mathematische Funktion ermöglicht zu jeder Zeit die Ableitung des Public Keys vom Private Key, der umgekehrte Weg (also die Erstellung des Private Keys mittels des Public Keys) würde die leistungsfähigsten Supercomputer mehrere Billionen Jahre beschäftigen. Der generierte Public Key steht auch anderen Nutzern zur Verfügung, und über diesen können Miner verifizieren, ob eine Transaktion tatsächlich von dem Wallet signiert wurde, von dem es vorgibt [Vos19, S. 41]. Aus dem Public Key wird zusätzlich mit einem differenzierten Algorithmus eine Blockchain-Adresse mit Meta-Informationen generiert. Der Algorithmus dient als zweite Sicherungsschicht, für den Fall dass der erste Algorithmus irgendwann mittels Quantencomputern geknackt werden kann. Die Blockchain-Adresse wird wie eine Bankkontonummer verwendet und dient zur eindeutigen Identifikation des Wallet [Vos19, S. 42]. Entgegen dem allgemeinen Glauben werden jedoch keine Tokens im Wallet gespeichert. Im Beispiel von Bitcoin heißt dass, das im Wallet keine Bitcoins selbst gespeichert sind. An dieser Stelle ist der Begriff Wallet nicht sehr treffend gewählt, denn darin werden nach dem Private- und Public-Key-Pair alle Transaktionen gespeichert, in denen der Public Key verwendet wurde.

Um den Prozess noch einmal abzubilden: Das Wallet (eine Software) enthält Private und Public Key, die Blockchain-Adresse und einige weitere Informationen für spezielle Transaktionen. Zusätzlich werden Einträge gespeichert, die Transaktionen mit dem eigenen Public Key enthalten [Vos19, S. 42]. Wird nun eine Transaktion ausgeführt, wird diese auf dem eigenen Gerät mit dem Private Key signiert. Diese signierte Transaktion nennt man *Digital Signature*. Ein anderer Netzwerkteilnehmer kann nun mit der Transaktion und dem Public Key des Senders verifizieren, dass es sich wirklich um denjenigen handelt, der er vorgibt zu sein. Erst nach erfolgreicher Identifikation und Verifizierung wird die Transaktion in die Blockchain geschrieben und an alle anderen Teilnehmer im Netzwerk verteilt. Die Transaktion kann nun nicht mehr verändert werden.

[7] Unter diesem Pseudonym wurde im Jahr 2008 das White Paper *Bitcoin: A Peer-to-Peer Electronic Cash System* veröffentlicht, bislang ist unklar ob es sich um eine einzelne Person oder ein Kollektiv von Personen handelt [BTC18]

4.1.5 Smart Contracts

Smart Contracts sind einem normalen Vertrag ziemlich ähnlich: Zwischen zwei oder mehreren Vertragspartnern geschlossene Vereinbarungen werden darin festgehalten. Dies geschieht jedoch nicht auf Papier, sondern in Form von Programmcode, der in der Blockchain ausgeführt wird. Genau wie die Blockchain selbst ist auch ein Smart Contract Open Source, und auch er kann nachträglich nicht mehr geändert werden. Verträge können somit nicht mehr so leicht verletzt werden. Ein weiterer großer Vorteil ist, dass bestimmte Aktionen automatisch ausgeführt werden können, ohne manuelles Eingreifen zu benötigen. Als Beispiel werden oft Lieferketten angeführt: Über die automatische Sendungsverfolgung kann zum Beispiel der Kaufbetrag automatisch überwiesen werden, wenn die Ware beim Kunden ankommt. Des weiteren fallen bei Smart Contracts zusätzliche Kosten weg, wie beispielsweise die eines Notars. Durch die Dezentralisierung der Verträge ist sichergestellt, dass dieser auch eingehalten wird, und handelsübliche, rechtskräftige Verträge werden nicht mehr benötigt.

Die bekannteste Plattform für die Nutzung von Smart Contracts ist die Plattform *Ethereum*. Diese ermöglicht die Nutzung und Erstellung sogenannter *Dapps*, was für *Distributed Apps* steht (zu deutsch: dezentrale Anwendungen). Durch diese Anwendungen können Smart Contracts erstellt und auf der Blockchain ausgeführt werden [Eth19b]. Zudem entstehen zunehmend Anwendungen, die die einfache Erstellung solcher Smart Contracts über eine Oberfläche ermöglichen, sodass auch nicht-Programmierer die Möglichkeit haben, an diesen teilzuhaben.

4.2 Konzept der Dezentralisierung im Web3

Doch wie findet nun die Technologie der Blockchain Einsatz in der nächsten Generation des Webs? Da die Blockchain maßgeblich im Zuge der Erfindung der Kryptowährung Bitcoin bekannt geworden ist und diese kontrovers diskutiert wird [CNP+16], werfen viele die zugrunde liegende Blockchain-Technologie oft mit der Währung in einen Topf. In Wirklichkeit dient sie jedoch für Bitcoin (und andere Kryptowährungen) nur als Mittel zum Zweck, und funktioniert seit deren Einsatz einwandfrei [CNP+16]. Nichtsdestotrotz denken viele Menschen bei dem Term Blockchain sofort an eine Kryptowährung. Dadurch fällt es schwer, sich auch andere Einsatzgebiete für die Technologie vorzustellen, beziehungsweise wie dieses Konzept aussehen soll. Dazu muss man nun das zuvor erläuterte Konzept der Dezentralisierung mit der Technik der Blockchain in Verbindung bringen: Computer oder Smartphones, wie sie heute bereits in Massen existieren, bilden auf der untersten Ebene die Netzwerkgeräte, die untereinander verknüpft sind. Mit einem darauf aufbauenden Blockchain-Netzwerk können nun verschiedenste Aufgaben erledigt und Dienste angeboten werden, die in Form von den beschriebenen Transaktionen ablaufen. Wichtig dabei ist, dass diese Blockchain-Netze grundlegend auf Tokens aufbauen. Im Beispiel von Bitcoin oder Ethereum sind die Tokens die Währung, in der gehandelt wird. Das Bitcoin-Netzwerk nutzt eine gleichnamige Währung (Bitcoin, abgekürzt BTC), im Fall von Ethereum ist die Währung Ether (oder ETH). Tokens sind jedoch ein allgemeines Konzept und unterscheiden sich von Netzwerk zu Netzwerk.

Tokens sind ebenfalls nicht zwingend eine Währung wie Bitcoin oder Ether, sondern sie können viel mehr Dinge repräsentieren. Shermin Voshmgir führt in ihrer Literatur 3 Arten von Tokens an: *Vermögenswerte* (zum Beispiel Strom in Kilowattstunden, Fiat-Währungen [8], Versicherungspolicen oder Event-Tickets), *Zugriffsrechte* (wie Softwarelizenzen, Mitgliedschaften oder Wahlrechte) und eine *Mischform* der beiden (Rechte zum "minen" oder native Tokens des jeweiligen Netzwerks (beispielsweise ETH oder BTC) [Vos19, S. 151]. Das heißt, dass eben nicht nur mit einer einzigen Währung bezahlt werden kann, sondern viele verschiedene Transaktionen ausgeführt werden können. Manche sprechen sogar von Beispielen, in denen ganze Autos oder Immobilien auf die Blockchain gehoben werden. Dadurch kann beispielsweise ein Testament als Smart Contract aufgelegt werden. Im Todesfall der betreffenden Person wird so das Vermögen auf die Erben verteilt, exakt so wie es im Smart Contract festgehalten ist [Kry18, 02:10].

So wichtig die Blockchain jedoch für das Web3 ist, kann sie allerdings mitnichten als Synonym für den Begriff dienen, wie es ab und zu bei Journalisten oder der Allgemeinheit der Fall ist [Vos19, S. 27]. Vielmehr ist Blockchain bloß eine Technologie von vielen, die in einem dezentralen Internet Einsatz finden. Um jedoch den Weg dorthin weitestgehend zu vervollständigen, werden einige andere Protokolle und Techniken benötigt,

[8] Fiat-Geld ist eine Währung, die keinen inneren bzw. festen Wert hat, so wie es bei Rohstoffen wie Gold oder Tabak der Fall ist [CAP18]. Von Zentralbanken ausgegebenes Geld wie Euro oder Dollar zählen ebenfalls zum Fiat-Geld.

um die heutigen Dienste mehr oder weniger abbilden zu können. Die Blockchain stellt in diesem Szenario einen großen Nutzen da, um in einem Peer-to-Peer-Netzwerk feststellen zu können, wer was und wann getan hat. Allerdings ist diese nicht dafür geeignet, große Datenmengen zu speichern und zu verarbeiten. Dies hat hauptsächlich 2 Gründe: Erstens sind Blockchains zu langsam und zu rechenintensiv, zweitens bietet die Blockchain nicht immer die richtigen Privatsphäre- und Datenschutzeinstellungen [Vos19, S. 27]. Zur Größeneinordnung: Die Blockchain des Bitcoin-Netzwerks stieg bis zum dritten Quartal im Jahr 2019 rasant auf eine Größe von knapp 250 GB [Blo19a].

Um nun das Web3 alltagstauglich einsetzen zu können, müssen wenigstens die folgenden Bereiche durch dezentrale Anwendungen abgedeckt werden [Vos19, S. 27]:

- Computerberechnungen
- Speicherplatz
- Kommunikation und Nachrichtenübermittlung
- Monetarisierung
- Zahlungsabwicklung

Die Blockchain-Technologie kann in diesem Konstrukt mit einem Prozessor in einem Rechner verglichen werden. Er ist für die grundlegende Funktionalität essentiell, benötigt jedoch noch andere Komponenten, ohne die das System nicht anwendbar wäre.

Mittlerweile gibt es bereits viele dezentrale Anwendungen, die als Lösungen für die oben genannten Komponenten dienen können [gda19]. Viele Protokolle und Plattformen sind noch in der Entwicklung, diese werden jedoch von Zeit zu Zeit besser, indem vor allem zunehmend Unternehmen in diesem Bereich forschen und Entwickeln. Dies belegt vor allem die steigende Zahl der weltweit gegründeten Unternehmen und Start-Ups in dieser Sparte seit 2013 [IPl19].

Einige dieser Projekte werden im nächsten Kapitel vorgestellt. Der Fokus liegt dabei darauf, wie diese dezentralen Anwendungen heutige Dienste und Plattformen abbilden oder sogar durch ein neues Konzept ersetzen können.

4.3 Dezentralisierung an Alltagsbeispielen erklärt

Die Beispiele sind in verschiedene Kategorien unterteilt, die allesamt dezentralisiert sind und teilweise sogar aufeinander aufbauen, um eine umfassende Web3-Umgebung zu konzipieren.

Abbildung 4. Logo des IPFS-Protokolls [Pro19]

4.3.1 Protokolle und Technologien

Protokolle und Technologien im Web3 basieren zum Teil auf Blockchain und sollen dabei helfen, verschiedenste dezentrale Anwendungen zu entwerfen und in den Web3-Stack zu implementieren.

IPFS | InterPlanetary File System Das IPFS ist ein Peer-to-Peer-Dateisystem, das den Anspruch erhebt, das HTTP-Protokoll abzulösen [Ide18]. In diesem Netzwerk werden Dateien über einen kryptographischen Hash eindeutig identifiziert und auf Netzwerk-Nodes (also einzelne Rechner im Netzwerk) verteilt. Das Konzept orientiert sich dabei an dem Protokoll BitTorrent, das ebenfalls auf den serverlosen Dateiaustausch zwischen Peers setzt. Die Dateien selbst werden jedoch auf jedem der Peers (oder Nodes) in einem Git Repository verwaltet und unterstützen Versionierung [Ide18]. Und auch wenn BitTorrent und weitere Protokolle der gleichen Kategorie wie Napster oder KaZaA sehr große Durchsatzraten besitzen, so sind sie dennoch nicht als Infrastruktur ausgelegt [Ben14].

An diesem Punkt setzt IPFS an, das zwar genau wie HTTP auf TCP/IP aufsetzt, jedoch nicht alleine von diesem Netzwerk-Protokoll abhängig ist. Der größte Vorteil gegenüber HTTP liegt dabei in der Verteilung von vor allem großen Dateien. Diese können sogar in Teilen von verschiedenen Nodes abgerufen werden und sind somit nicht von einer einzigen Bandbreite abhängig. Dieses bietet auch im Streaming enorme Vorteile, vor allem wenn die Datei stark frequentiert ist. Durch das Abrufen eines Videos beispielsweise wird die Datei zur Wiedergabe auf das eigenen Gerät heruntergeladen. Dadurch wird diese jedoch gleichzeitig auch anderen Netzwerkteilnehmern zur Verfügung gestellt, die eventuell sogar geographisch einen kürzeren Abstand besitzen und die Dateien somit nicht mehr um die ganze Welt geschickt werden müssen. Dies funktioniert,

Abbildung 5. Logo-Schriftzug der Bigchain-Datenbank [Vec19]

da IPFS Inhalte (also Dateien) über deren Hash-Werte adressiert, und nicht wie HTTP über Speicherorte. Wird eine Website über HTTP(S) über einen Domainnamen aufgerufen, wird dieser Name über ein Domain Name System zu einer IP-Adresse und einem Speicherort auf dem adressierten Server aufgelöst. Bei IPFS hingegen sucht sich das Netz bei einem Dateiaufruf die am nächsten gespeicherte Datei, was einen enormen Geschwindig-keitsvorteil darstellt und zusätzlich Ausfallsicherheit gewährleistet [Cod19] Davon abgesehen ist auch ein Dateizugriff möglich, wenn bestimmte Netzwerk-Bereiche durch beispielsweise Zensur oder Naturkatastrophen abgeschnitten sind [Ide18].

Sidenote: *Nachdem die Zentralregierung in Madrid verschiedene Domains hat sperren lassen, die zur Organisation des katalanischen Referendums zur Unabhängigkeit dienten, veröffentlichte der katalanische Präsident Puigdemont einen Link auf eine Datei in einem IPFS-Netzwerk [Win17]. Da heutige Browser das IPFS-Protokoll noch nicht implementiert haben, muss der Dateiaufruf über einen Webserver auf HTTP umgeleitet werden [Ide18], die Datei selbst mit Informationen über das Referendum am 01. Oktober 2017 war jedoch in einem dezentralen Netz verfügbar.*

Blockstack Blockstack ist ein dezentrales Internet und bietet eine Plattform für die Entwicklung dezentraler Apps und verschiedensten Öko-Systemen. Die beiden Gründer des New Yorker Unternehmens, Muneeb Ali und Ryan Shea, wollen damit gegen die Macht, Einflussnahme und Vorherrschaft der GAFA-Konzerne [9] vorgehen [Kyr18]. Der Schwerpunkt liegt dabei auf Datensicherheit durch Verschlüsselung und Privatsphäre. Da alle Daten verteilt und nicht auf einem zentralen Server gespeichert sind, hat der Nutzer ständige Kontrolle, inklusive der vollständigen Löschung seiner gesamten Daten [Kyr18].

4.3.2 Databases

[9] **G**oogle, **A**pple, **F**acebook und **A**mazon

BigchainDB Die vom Berliner Startup *Ascribe* ins Leben gerufene Datenbank BigchainDB setzt ebenfalls auf die Blockchain-Technologie. Sie soll, wie andere dezentrale Anwendungen auch, "dezentralisierte Kontrolle, Widerstandsfähigkeit gegen Manipulationen [sowie] Erzeugung und Übertragung von Werten" [Sch16] bieten. Dabei deckt sie ein weitläufiges Einsatzgebiet ab, sowohl für Privatpersonen als auch für Unternehmen. Dazu zählen unter anderem [Sch16]:

- **Verbindliche Verträge** mit allen dazugehörigen Transaktionen können direkt in der BigchainDB gespeichert werden.
- **Erzeugung und sofortige Übertragung von großen Vermögen.** Nur der Besitzer der Vermögen kann diese übertragen. Nicht der Netzwerkadministrator, wie in bisherigen Datenbanksystemen. Kosten werden minimiert, alles soll schneller gehen.
- **Echtzeit-Verfolgung der Produktion von Gegenständen.** Zum Beispiel indem Daten von RFID-Chips in Bigchain gespeichert werden. So sollen Kosten gespart und Betrug vermieden werden.
- **Nachhalten von Urheberrechten.** Digitale Kunstwerke oder Musik kann mit einem Wasserzeichen versehen werden. Alle Informationen über die Verbreitung und Kopien werden dann in der Bigchain gespeichert. Der Lizenzinhaber behält den Überblick über die Verbreitung seiner Werke. Auf dieses Feld hat sich Ascribe konzentriert.
- **Zeitstempel, Zertifikate und Quittungen.** Bigchain ist in der Lage, digitale Vorgänge offen zu legen. Wann wurde was übertragen? Das verhindert juristische Probleme bei Vertragsabschlüssen.
- **Verbesserung der Verlässlichkeit von Datenbanken.** Bis jetzt kann ein einziger Fehler zu Datenlecks führen. BigchainDB kann das verhindern.

Der größte Vorteil liegt jedoch zweifelsohne in der Geschwindigkeit: Durch den dezentralen Ansatz soll die Datenbank in der Lage sein, mehr als eine Million Vorgänge pro Sekunde abzuarbeiten. Dies ermöglicht die hohe Skalierbarkeit, die zu Anfang des Produkts nicht gegeben war [Sch16].

IPDB | InterPlanetary Database Nicht zu verwechseln mit der *Internet Pinball Machine Database* (erreichbar unter ipdb.org) verspricht die Webseite unter ipdb.io eine neue Datenbank für das dezentrale Web. Die von *The Interplanetary Databse (IPDB) Foundation e.V.*, einer deutschen Non-Profit-Organisation, ins Leben gerufene Datenbank baut auf der zuvor beschriebenen BigchainDB und dem IPFS auf [IPD18]. Das Projekt wird derzeit von einem Konsortium von Organisationen unterstützt, die die Idee einer gut verwalteten Blockchain-Datenbank unterstützen [IPD18]. Shermin Voshmgir sieht diese Datenbank hauptsächlich im Gebiet der Metadaten-Speicherung in einem P2P-Netzwerk [Vos19, S. 29].

4.3.3 Datenspeicherung und -freigabe

Storj Diese im Jahr 2014 als Open-Source gegründete Plattform ist die dezentrale Dropbox (oder Google Drive). Storj wird in diesem Fall wie SStorageäusgesprochen [Blo19c]. Das in Atlanta ansässige Unternehmen Storj Labs bietet sein Produkt im Prinzip als zweiseitige Medaille an. Auf der einen Seite stehen die sogenannten *Farmer*, die eigenen Speicherplatz bereitstellen und dafür entlohnt werden. Wer nun eigene Dateien in der Cloud speichern möchte, mietet sich dafür einfach Speicherplatz. Dieser Speicherplatz wird jedoch nicht auf einem einzigen Geräte bereitgestellt, vielmehr werden die hochgeladenen Dateien in Fragmente, sogenannten *Shards*, unterteilt und auf viele verschieden Farmer verteilt [Blo19c].

Sidenote: *Ein Farmer in einem Storj-Netzwerk kann auch als Node oder Peer bezeichnet werden.*

Hauptaugenmerk bei dieser Anwendung liegt auf der Ende-zu-Ende-Verschlüsselung und die Fragmentierung der einzelnen Dateien. Selbst wenn es einem Angreifer gelingen würde, die Verschlüsselung zu knacken, hätte er nur ein Fragment der Datei, und ohne die Speicherorte der anderen Fragmente kann die Datei kaum gelesen werden. Die Information über die Speicherorte der einzelnen Fragmente besitzt jedoch nur der Eigentümer der Datei, was einen Höchstgrad an Sicherheit garantiert [Blo19c].

Sia Das Konzept des Speicheranbieters Sia ist dem von Storj sehr ähnlich. Hier besitzt ein Nutzer der Cloud sogar einen eigenen privaten Chiffrierschlüssel. Der Zugriff auf die Dateien erfolgt automatisch mittels einem Smart Contract, was zusätzliche Sicherheit gewährt. Zudem gilt auch hier, dass niemand anderem (vor allem einer fremden Person oder einem fremden Unternehmen) vertraut werden muss, und trotzdem sind die Daten redundant und damit ausfallsicher in der Cloud abgelegt [Sia19].

Swarm Diese verteilte Speicherplattform setzt auf dem Web3-Stack der Plattform Ethereum auf, und ermöglicht Entwicklern die Nutzung von redundantem Speicher, etwa für Dapp-Code, Benutzerdaten oder Metadaten zur Blockchain [Swa19]. Swarm ist Teil der Roadmap von Ethereum hin zu einem dezentralen Internet. Es existiert dabei neben Smart Contracts und Whisper als dezentrale Nachrichtenübermittlung und stellt daher einen essentiellen Part dar [Ger16].

Abschließend lässt sich festhalten, dass es eine zunehmende Anzahl von dezentralen Netzwerken und Anwendungen gibt, die mehr oder weniger auf Blockchain basieren. In folgendem GitHub-Repository von *gdamdam* (https://github.com/gdamdam/awesome-decentralized-web) ist eine Liste von dezentralen Technologien zu finden, die noch immer erweitert wird.

4.4 Vor- und Nachteile

Recap: Viele Vorteile des dezentralen Webs wurden bereits in den vorhergehenden Ausführungen angesprochen und erläutert, zur Vollständigkeit werden nachfolgend die Wichtigsten erneut aufgelistet:

- **Ausfallsicherheit:** In einem verteilten Netz gibt es keinen Single-Point-of-Failure, was erhöhte Datenverfügbarkeit in den meisten Bereichen mit sich bringt.
- **Schutz vor Angriffen:** Blockchain-basierte Netzwerke und Anwendungen besitzen viel höhere Sicherheitsmaßnahmen, beispielsweise durch starke Verschlüsselungsalgorithmen. Zudem können Angriffe nicht auf einen einzigen Server konzentriert werden, um beispielsweise Daten zu stehlen oder einen Ausfall zu verursachen.
- **Datenschutz und Privatsphäre:** Nutzer sind Eigentümer über die eigenen Daten und müssen diese keinen Intermediären anvertrauen. Sie haben bei korrekter Anwendung (wie zum Beispiel Geheimhaltung des Private Keys) die alleinige Kontrolle über die eigenen Daten, können frei über diese verfügen und sie gegebenenfalls löschen. Auch der Schutz vor Angriffen bewirkt eine enorme Senkung der Eingriffe in die Privatsphäre der Nutzer.

- **Keine Intermediäre:** Dieser Punkt birgt Vorteile in vielen Bereichen. Durch den Wegfall der Vermittlungsplattformen können enorme Kosten und Wege gespart werden, dies zudem bei höchstem Datenschutz.
- **Smart Contracts:** Bereits heute gibt es eine Vielzahl von Anwendungsfällen, die viele Vorgänge einfacher und sicherer gestalten können. Diesen ist nach oben hin keine Grenze gesetzt, und Smart Contracts haben die Möglichkeit, sowohl das Privatleben als auch die Prozesse von Unternehmen massiv zu verändern.

Diese Punkte jedoch so stehen zu lassen, wäre nicht korrekt, denn die Entwicklung dieser Protokolle und Anwendungen hat quasi gerade erst begonnen. Durch den Anstieg an Unternehmen, die sich in diesem Bereich angesiedelt haben, stehen mehr und mehr Ressourcen für Forschung und Entwicklung zur Verfügung, dennoch müssen viele Probleme erst noch gelöst, geschweige denn erkannt werden. Und auch wenn es für viele der heutigen Anwendungen bereits dezentrale Lösungen gibt, fehlt es dennoch an einer Auswahl an etablierten Netzen und Plattformen, um einen produktiven Einsatz zu gewährleisten.

Des Weiteren steht und fällt eine Anwendung mit ihrer Programmierung. Auch wenn Bugs heute bereits fatale Folgen haben können, ist die Entwicklung mit bekannten Techniken in den allermeisten Fällen serienreif, und immer beliebter werdende Test-Frameworks und -Prozesse sichern die korrekte Ausführung der Programme. Da viele dezentrale Projekte den Open-Source Ansatz verwenden, greift in diesen Fällen das Vier-Augen-Prinzip, was die Fehlersuche beschleunigen kann. Dennoch werden dafür auch genügend Entwickler benötigt, die dieser Aufgabe nachkommen und die dafür qualifiziert sind.

Vor allem bei den Smart Contracts können Programmierfehler ein hohes Risiko bergen. So verlässlich und automatisiert sie in ihrer Ausführung sind, so sicher werden eben auch Probleme bei falscher Programmierung verursacht, wie das folgende Beispiel zeigt.

Dem Wagniskapitalgeber *The DAO*, der im April 2016 mit 150 Millionen US-Dollar aus einer Crowdfunding-Kampagne startete, wurde dies zum Verhängnis. The DAO war eine **d**ezentrale, **a**utonome **O**rganisation (daher der Name), die mithilfe von Smart Contracts in Unternehmen, vor allem in Start-Ups investieren wollte. Der Unterschied zu anderen Venture-Capital-Firmen? Die Organisation kommt ohne Management oder Direktoren aus, stattdessen werden die Entscheidungen für Investitionen automatisch mit Smart Contracts getroffen [Rei19]. The DAO setzte auf Ethereum auf und benutzte dessen Währung ETH. Bereits im Juni des selben Jahres gelang es jedoch einem Nutzer, über einen längeren Zeitraum insgesamt Ether im Wert von ungefähr 50 Millionen US-Dollar auf sein eigenes Konto umzuleiten [Rei19]. Während die Gründer überlegten, wie sie das Geld zurückholen können, bekamen sie einen Brief des "Diebs", und darin drohte dieser The DAO mit rechtlichen Schritten! Er gelangte nämlich durch einen Programmierfehler eines Smart Contracts an die Tokens, und auch wenn sein Verhalten unethisch war, illegal war es nicht [Kry18, 05:08]. Letztendlich erhielt er das Geld nicht, dennoch führte der "Diebstahl"bereits im September 2016 zum Ende von The DAO [Rei19].

Das Ethereum-Netzwerk wurde einem Hard-Fork unterzogen. Das heißt es gibt derzeit 2 Versionen von Ethereum: Eine alte, in der der Programmierfehler immer noch existiert, und eine neue, wo der Fehler durch Updates der Ethereum Nodes behoben wurde. Und obwohl die Ethereum-Community mehrheitlich für den Hard-Fork gestimmt hatte, spaltete der Vorfall die Nutzerschaft, denn dieser sei nicht im Sinne eines führerlosen und dezentralen Systems [Hay16].

5 Ausblick

Nachdem nun die aktuelle Situation des heutigen Internets aufgezeigt und die möglichen Entwicklungen in der Zukunft erläutert wurden, soll das letzte Kapitel sich damit beschäftigen, inwieweit die Dezentralisierung im Bezug auf das Internet Einzug finden kann beziehungsweise wird.

Wie in Figure 6 zu sehen, befindet sich die Technologie *Decentralized Web* noch ziemlich am Anfang des Gartner Hype Cycle's, und der Zeitraum bis zur Etablierung ist auf 10 Jahre geschätzt. Wie bereits angesprochen, sieht man immer mehr Unternehmen, Organisationen und damit letztlich Menschen an der Technologie arbeiten. Dies liegt hauptsächlich daran, dass es die heutigen Tech-Konzerne mit der Verletzung der Privatsphäre zu weit getrieben haben. Letztendlich arbeiten viele Personen freiwillig an der Technologie, weil sie für ein freies Internet kämpfen, in dem die Nutzung von Diensten nicht mit seinen privaten Daten “erkauft“ wird. Denn nichts anderes passiert in der jetzigen Zeit des Web2: Die frühen Anbieter von Services im Internet haben sehr schnell mitbekommen, dass Nutzer nicht

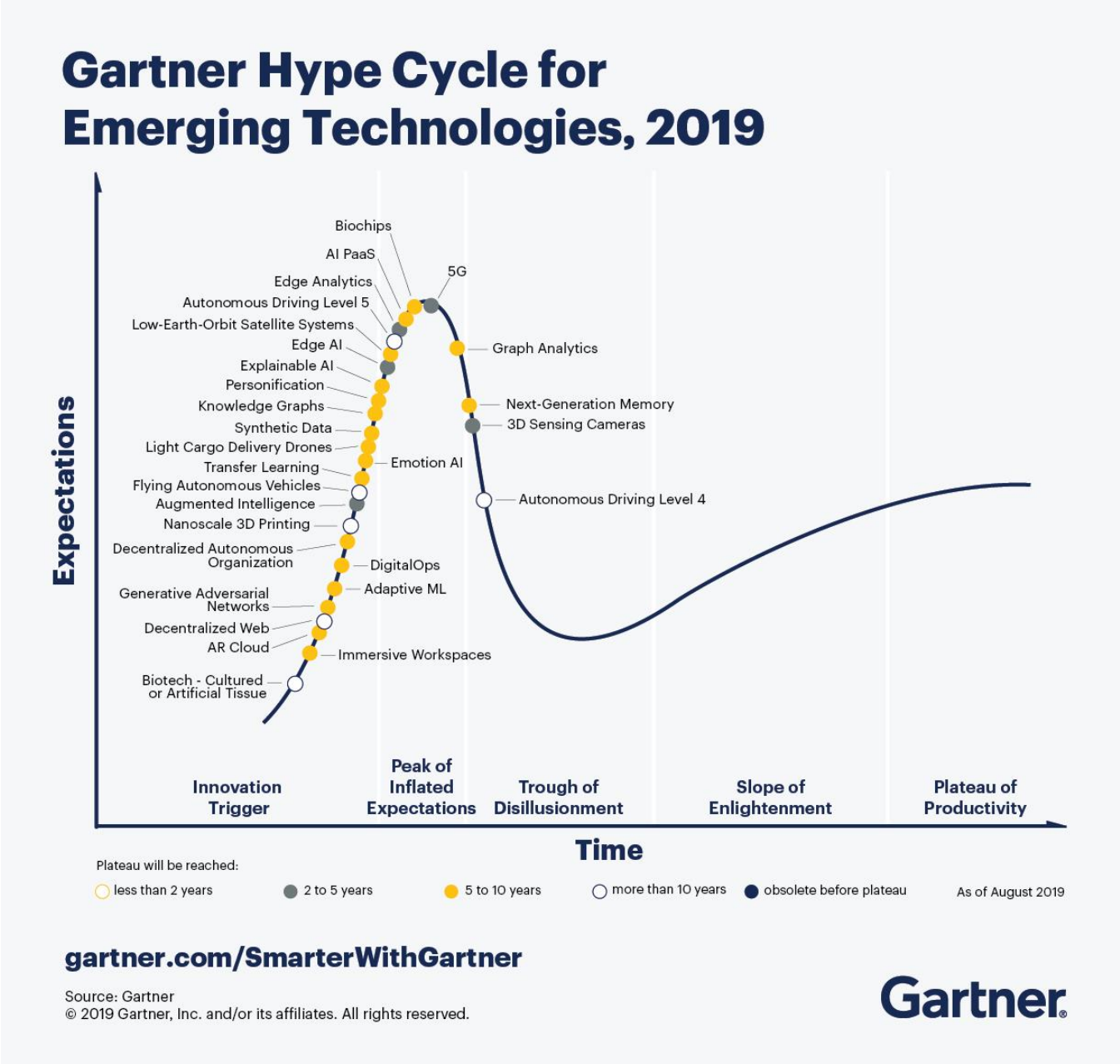

Abbildung 6. Gartner Hype Cycle for Emerging Technologies, 2019 [Pan19]

bereit dafür sind, für die Nutzung der Dienste im Web zu bezahlen. Also suchten sie nach anderen Möglichkeiten, Profit zu generieren, und dadurch entwickelte sich die heutige Kommerzialisierung mit Nutzerdaten.

Und dieses Konzept war nie im Sinne des Erfinders. Der durch seine Pionier-Arbeit am World Wide Web zum Ritter geschlagene Sir Timothy Berners-Lee hat nie auch nur ansatzweise ein Vermögen mit seiner Erfindung verdient, er wollte lediglich das Leben der Menschen verbessern und vereinfachen. Nun arbeitet er schon länger am sogenannten Solid-Projekt [Cla18]. Die Abkürzung steht für Social Linked Data und zielt darauf ab, den großen Technik-Firmen die Nutzerdaten aus ihren Daten-Silos zu entziehen und diese in sogenannten Pods zu speichern, die der Nutzer selbst

kontrolliert. So soll beispielsweise ein Umzug von Firma A zu Firma B problemlos möglich sein: Man entzieht A ganz einfach die Berechtigung auf den eigenen Datenpod und gewährt sie B [Par18].

Dies wird jedoch schwieriger, als auf den ersten Blick ersichtlich: Die Konzerne, gegen die das Projekt gerichtet ist, werden sich wohl kaum an einer einheitlichen Lösung beteiligen, und für neue oder kleine Firmen fehlt es an Nutzerzahlen und damit an Investoren [Par18]. Dieses Problem entstand laut Steven Johnson, weil die von ihm als "InternetOne" bezeichnete Schicht offene Protokolle wie TCP/IP und HTML verwendeten, und die Verwaltung von Identitäten und persönlichen Daten auf das "InternetTwo" ausgelagert wurden. Die Protokolle dieser zweiten Schicht wurden jedoch vornehmlich von Unternehmen definiert, weshalb kaum Standards im Bereich der Datensicherheit existieren [Bon19].

All das Engagement zeigt, dass vor allem das Thema der Privatsphäre und des gläsernen Bürgers in den Vordergrund rückt. Doch eine schnelle Änderung der Situation wird dies wohl nicht bewirken, dafür verzeichnen die etablierten Plattformen zu große Nutzerzahlen, und es gibt noch zu wenige beziehungsweise keine konkurrenzfähigen Alternativen.

Vermutlich werden in der Zukunft Unternehmen die Technologie der Dezentralisierung weiter vorantreiben und auch einsetzen, bevor diese vollumfänglich in den privaten Sektor vordringt. Denn durch die Blockchain stehen vor allem Unternehmen enorm viele Möglichkeiten offen, da diese nicht nur Prozesse vereinfachen und automatisieren kann, sondern auch hohe Kostensenkungen ermöglicht.

Fakt ist, dass die Technologie noch viele Jahre zur Marktreife benötigt. Nichtsdestotrotz stellt sie jedoch eine realistische Alternative zum Marktmonopol einiger weniger Unternehmen dar, und diese Alternative wird mit zunehmenden Jahren immer dringender benötigt. Die Veränderung zum dezentralen Web wird jedoch nach und nach Anklang finden, je nachdem wie die Entwicklung voranschreitet und die Technik in der Gesellschaft angenommen wird.

Literatur

[Ben14] Benet, Juan: *IPFS - Content Addressed, Versioned, P2P File System*. http://arxiv.org/pdf/1407.3561v1. Version: 2014

[Blo19a] Blockchain ; Statista - Das Statistik-Portal (Hrsg.): *Bitcoin blockchain size 2010-2019*. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/. Version: 2019

[Blo19b] Blockchainhub.net: *Web3 - The Decentralized Web*. https://blockchainhub.net/web3-decentralized-web/. Version: 2019

[Blo19c] Blockchainwelt: *Storj - die dezentrale Speicherplattform*. https://blockchainwelt.de/storj-dezentrale-speicherplattform/. Version: 2019

[Bon19] Bonset, Sébastien ; t3n (Hrsg.): *Web 3 – der Anfang vom Ende der Plattformökonomie ist dezentral*. https://t3n.de/news/web-3-der-anfang-vom-ende-der-plattformoekonomie-ist-dezentral-982153/. Version: 2019

[BSZ16] Beutelsbacher, Stefan ; Sommerfeldt, Nando ; Zschäpitz, Holger ; WELT (Hrsg.): *Die gefährliche Dominanz der großen Vier*. https://www.welt.de/finanzen/article150809163/Die-gefaehrliche-Dominanz-der-grossen-Vier.html. Version: 2016

[BTC18] BTC Academy: *Wer ist Satoshi Nakamoto?* https://www.btc-echo.de/academy/bibliothek/wer-ist-satoshi-nakamoto/. Version: 2018

[CAP18] CAPinside: *Was bitte sind FIAT-Währungen? - Eine kurze Einführung*. https://capinside.com/contents/was-bitte-sind-fiat-waehrungen-eine-kurze-geschichte. Version: 2018

[CER20] CERN: *The birth of the Web | CERN*. https://home.cern/science/computing/birth-web. Version: 2020

[Cis11] Cisco Systems ; Statista - Das Statistik-Portal (Hrsg.): *Anzahl vernetzte Geräte weltweit bis 2020 I Prognose | Statista*. https://de.statista.com/statistik/daten/studie/479023/umfrage/prognose-zur-anzahl-der-vernetzten-geraete-weltweit/. Version: 2011

[Cla18] Clark, Kate: *Tim Berners-Lee is on a mission to decentralize the web*. https://techcrunch.com/2018/10/09/tim-berners-lee-is-on-a-mission-to-decentralize-the-web/. Version: 2018

[CNP+16] Crosby, Michael ; Nachiappan ; Pattanayak, Pradan ; Verma, Sanjeev ; Kalyanaraman, Vignesh: BlockChain Technology: Beyond Bitcoin. (2016). https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

[Cod19] CodersBlog.de: *Einführung in das IPFS (InterPlanetary File System)*. http://www.codersblog.de/einfuehrung-in-das-ipfs-interplanetary-file-system/. Version: 2019

[Dud19] Duden: *Duden | Killerapplikation | Rechtschreibung, Bedeutung, Definition, Herkunft*. https://www.duden.de/rechtschreibung/Killerapplikation. Version: 2019

[Eth19a] Ethereum: *Ethereum.org*. https://ethereum.org/de/. Version: 2019

[Eth19b] Ethereum: *web3.js documentation*. https://web3js.readthedocs.io/en/v1.2.4/. Version: 2019

[Fie16] Fiedler, Maria: *Wie Tim Berners-Lee das Web erfand*. https://www.tagesspiegel.de/gesellschaft/25-jahre-www-wie-tim-berners-lee-das-web-erfand/13946806.html. Version: 2016

[gda19] gdamdam: *Awesome Decentralized Web*. https://github.com/gdamdam/awesome-decentralized-web. Version: 2019

[Ger16] Gerring, Taylor ; Ethereum Stack Exchange (Hrsg.): *What is Swarm and what is it used for?* https://ethereum.stackexchange.com/questions/375/what-is-swarm-and-what-is-it-used-for. Version: 2016

[Hay16] Hayes, Adam: *Why are There Now Two Ethereums?* https://www.investopedia.com/articles/investing/080516/why-are-there-now-two-ethereums.asp. Version: 2016

[Hel02] Held, G.: *The ABCs of TCP/IP*. Taylor & Francis, 2002 https://books.google.de/books?id=AvC4qJ7oPtIC. – ISBN 9781439832301

[Hil] Hilz, Jascha: *Semantic Web: Definition & Grundlagen*. https://www.advidera.com/glossar/semantic-web/

[Hor17] Horizont ; Statista - Das Statistik-Portal (Hrsg.): *Datenschutz - Vertrauen in Internetunternehmen in Deutschland 2017 | Statista*. https://de.statista.com/statistik/daten/studie/790373/umfrage/vertrauen-in-den-datenschutz-von-internetunternehmen-in-deutschland/. Version: 2017

[Ide18] Ideas Engineering: *Das Interplanetary File System (IPFS)*. https://www.ideas-engineering.io/blog/2018/10/inter-planetary-file-system. Version: 2018

[IPD18] IPDB: *IPDB Foundation Assumes Governance of BigchainDB Software and Testnet*. https://medium.com/ipdb-blog/ipdb-foundation-assumes-governance-of-bigchaindb-software-and-testnet-51235322e14c. Version: 2018

[IPl19] IPlytics GmbH ; Statista - Das Statistik-Portal (Hrsg.): *Blockchain-Unternehmen und Start-ups weltweit - Anzahl der jährlichen Gründungen bis 2018*. https://de.statista.com/statistik/daten/studie/1062771/umfrage/anzahl-der-pro-jahr-gegruendeten-blockchain-unternehmen-und-start-ups-weltweit/. Version: 2019

[ITW17] ITWissen.info: *SPoF (single point of failure)*. https://www.itwissen.info/SPoF-single-point-of-failure.html. Version: 2017

[KPR17] Kneisel, Peter ; Priefer, Dennis ; Rost, Wolf ; IIS (Hrsg.): *3-Wege-Handshake: Webbasierte Programmierung 2*. 2017

[Kra08] Krause, Maike ; Planet Schule (Hrsg.): *Timothy Berners-Lee und das World Wide Web*. https://www.planet-schule.de/wissenspool/meilensteine-der-naturwissenschaft-und-technik/inhalt/hintergrund/technik/timothy-berners-lee-und-das-world-wide-web.html. Version: 2008

[Kry18] Krypto: *Was sind Smart Contracts? Intelligente Verträge einfach in 6 Minuten erklärt!* https://www.youtube.com/watch?v=SOXLWNPP8d0. Version: 2018

[Kyr18] Kyriasoglou, Christina: *Diese Gründer bauen mit der Blockchain ein neues Internet*. https://www.gruenderszene.de/allgemein/blockstack-blockchain-shea-internet. Version: 2018

[LD18] Luber, Stefan ; Donner, Andreas ; IP Insider (Hrsg.): *Was ist Peer-to-Peer (P2P)?* https://www.ip-insider.de/was-ist-peer-to-peer-p2p-a-654713/. Version: 2018

[Pan19] Panetta, Kasey: *5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019*. https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019. Version: 2019

[Par18] Park, Enno: *Solid: Wie WWW-Erfinder Tim Berners-Lee ein neues, besseres Internet plant*. https://t3n.de/news/solid-www-erfinder-tim-955024/. Version: 2018

[Pro19] Protocol Labs: *IPFS Project*. https://protocol.ai/projects/#IPFS. Version: 2019

[Rei19] Reiff, Nathan: *What Is the DAO?* https://www.investopedia.com/tech/what-dao/. Version: 2019

[Sch16] Schmiechen, Frank: *Hier ist die Blockchain für alle*. https://www.gruenderszene.de/allgemein/blogchain-bigchain-nerdstuff. Version: 2016

[shi18] shivang: *Difference Between Centralized, Decentralized & Distributed Systems Oversimplified*. https://www.8bitmen.com/difference-between-centralized-decentralized-distributed-systems-explained/. Version: 2018

[Sia19] Sia: *Sia*. https://sia.tech/. Version: 2019

[Swa19] Swarm: *Swarm*. https://swarm.ethereum.org/. Version: 2019

[Swe16] Sweeney, Peter: *The History of the Semantic Web is the Future of Intelligent Assistants*. https://medium.com/inventing-intelligent-machines/the-history-of-the-semantic-web-is-the-future-of-intelligent-assistants-da2ed50443be#.42y81yn1x. Version: 2016

[Vec19] Vecta.io: *BigchainDB icon*. https://vecta.io/symbols/75/brands-ba-bz/57/bigchaindb. Version: 2019

[Vos19] Voshmgir, Shermin: *Token economy: How blockchains and smart contracts revolutionize the economy*. 1st edition, 2nd amended printing. 2019. – ISBN 978–3982103822

[Web19a] Web3 Foundation: *About Web3 Foundation*. https://web3.foundation/about/. Version: 2019

[Web19b] Web3 Summit: *Web3 Summit 2019*. https://web3summit.com/. Version: 2019

[Wel19] Weltmaschine.de: *CERN*. https://www.weltmaschine.de/cern_und_lhc/cern/. Version: 2019

[Win17] Winters, Rainer ; ANA LOGO (Hrsg.): *Katalonien veröffentlicht neuen Link für Referendum 1-0*. https://analogo.de/2017/09/23/katalonien-veroeffentlicht-neuen-internetlink-fuer-referendum-1-0/. Version: 2017