FOM Hochschule für Ökonomie und Management

Hochschulzentrum München

Seminararbeit

Im Rahmen des Moduls

Fallstudie / Wissenschaftliches Arbeiten

Über das Thema

Big Data versus Blockchain
Wie sehen die Internetdienstleistungen der Zukunft aus?

von

Leonardo Ciria Buil

Gutachter: Dr. Herbert Bauer
Matrikelnummer: 604431
Abgabedatum: 10.01.2022

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BAT Basic Attention Token.

BTC Bitcoin.

P2P Peer-to-Peer.

1 Einleitung

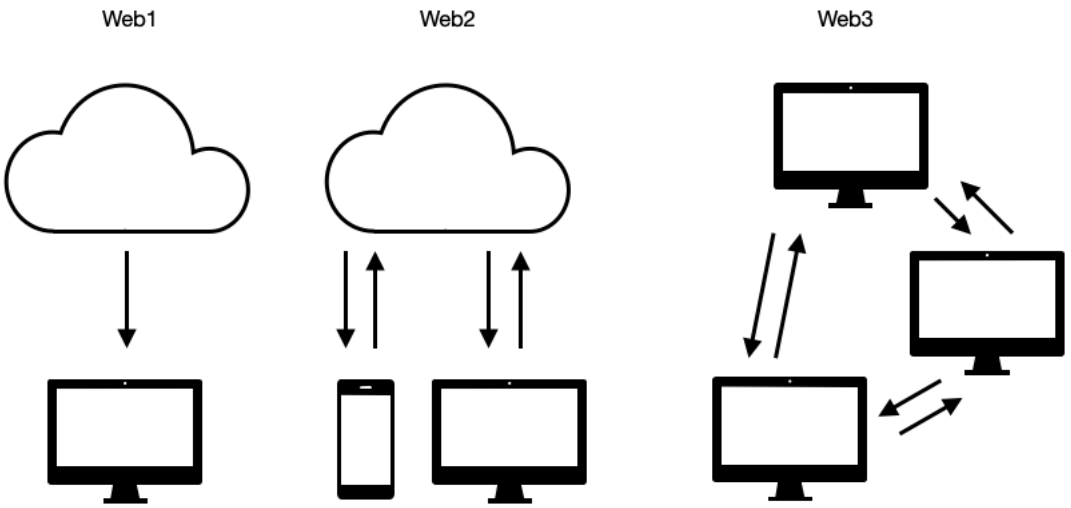
1.1 Geschichte des Internets

„This is a fantasy documentary. The pioneering work shown in Hyperland however, is very real.“ [5] Mit diesen Worten beginnt Dougles Adams 50-minütige Dokumentation aus dem Jahre 1990 mit dem treffenden Titel „Hyperland“. Der renommierte Science-Fiction-Autor stellt in diesem Dokumentarfilm dar, wie ein Internet mit (Hyper-)Links interaktiv navigierbar wäre, und dies Jahre vor den ersten Browsern. Im darauffolgenden Jahr entwickelte Tim Berners-Lee das World Wide Web, welches bald einen neuen Standard fürs Internet setzen sollte. Dieser Standard erleichterte das Programmieren der einzelnen Internetseiten, sowie die Navigation zwischen den einzelnen Seiten selbst, und das durch nicht mehr als einen Klick dank der Einführung eines Standards für die Erstellung visueller Webseiten ein (Hypertext).[4, Seite 379] Diese Version des Internets ist heutzutage als Web 1.0 bekannt und, auch wenn dies damals noch nicht vorherzusehen war, prägte es die Vielfältigkeit und Sinnvollheit, wozu sich das Internet entwickeln würde.

In weniger als einem Jahrzehnt würde sich das Internet noch ändern. Die Ära des Web 2.0 ist geprägt von vielen Technologien und Innovationen, sowie von der Idee, dass der Nutzer immer weniger eine ausschließliche Rolle als passiven Konsumenten einnehmen soll, sondern vielmehr die doppelte Rolle des Konsumenten in einigen Bereichen und des Produktes in anderen, aber auch die des Anbieters, da immer mehr Anwendungen aus dem Web 2.0 dem Laien erlaubten, Inhalte selbst zu erstellen, zu bearbeiten und zu verteilen. Um diese neue Rolle zu definieren, hat sich der Begriff Prosument (aus dem Englischen Prosumer) durchgesetzt. *„Versammle eine Menge an Leuten, die glauben, sie seien wegen der einen Sache dort, in Wirklichkeit aber wegen einer ganz anderen Sache da sind.“* [1, Seite 51] Eine der prägnantesten Innovationen dieser Internet-Epoche ist die Weiterentwicklung der Serveranbindung, aber auch neue Formen von Sicherheit, sowie Technologien, welche die Kommunikation zwischen dem Computer eines Nutzers und dem Server auf verschiedene Arten verbessern. Wegen der immensen Anzahl an Informationen, welche durch diese zentralisierte Server fließen, spricht man allgemein von „Big Data“. Dieser Begriff soll später noch genauer erklärt werden.

Doch auch diese Zeit scheint sich langsam dem Ende zu neigen. Und damit ist die Zeit reif für den Anbruch des Web 3.0. Beim Web 3.0 steht hauptsächlich die Idee im Vordergrund, dass das Internet dezentral über Peer-to-Peer-Netzwerke laufen soll.[4, Seite 42] Das wohl verbreiteste Beispiel hierfür wären die Blockchain-Netzwerke. Diese neue Erfindung bringt jedoch eine Reihe von technischen und rechtlichen Herausforderungen mit sich, und in vielen Ländern ist das Wissen über die Mechanismen, Möglichkeiten und Risiken des Web 3 noch unzureichend. Hinzu kommt, dass viele der Mechanismen noch in den Kinderschuhen stecken und für viele Menschen zu abstrakt erscheinen. Worte wie Kryptowährung, Smart Contracts und Token sind allgegenwärtig, aber es gibt immer noch einen Mangel an Informationen über die Mechanismen hinter diesen Anwendungen und den aktuellen Stand der Technik.

Bild 1: 3 Epochen des Internets



Quelle: Token S. 19

1.2 Forschungsziel, Forschungsfrage und These

1.2.1 Forschungsziel

Wenn man von Distributed Ledger Systemen hört, wie beispielsweise dem Blockchain-Netzwerk, ist überwiegend von den positiven Aspekten sowie dem Potenzial, welches diese anbieten, die Rede. *„Jede Technologie ist aber lediglich ein Werkzeug und zunächst neutral. Wie wir dieses Werkzeug einsetzen, ist fast nie eine technologische, sondern immer mehr eine humanistische Frage.“* [4, Seite 25] Im Folgenden soll zunächst ein Überblick über die Grundlagen der Technologien von Big Data und Blockchain gegeben werden. Anschließend sollen beide verglichen werden. Ziel dieser Arbeit ist herauszufinden, ob es als plausibel erscheint, dass Big Data durch Blockchain ersetzt werden soll, und falls ja, welche Zeitspanne dafür denkbar wäre.

1.2.2 Forschungsfrage

Welche Vor- und Nachteile haben die beiden Strukturen (BigData und Blockchain) und wie zukunftstauglich sind sie?

1.2.3 These

Im Laufe der kommenden 10 Jahren wird Blockchain die meisten zentralen Systeme ersetzt haben.

1.3 Aufbau der Arbeit

Die vorliegende Arbeit unterteilt sich in mehrere Abschnitte. Zuerst werden die beiden Datenbanksysteme und deren jeweiliger Aufbau sowie der derzeitige Stand der Technik anhand von Anwendungsmöglichkeiten erklärt. Daraufhin werden beide Netzwerktypen auf mehrere Charakteristika untersucht. Aufgrund dessen wird schließlich auf die Umsetzungswahrscheinlichkeit auf Blockchain, sowie auf die Zukunfttauglichkeit beider geschlossen. Zuletzt trifft der Autor ein Urteil und gibt seine Meinung zu der Frage, ob und, wenn ja, wann Blockchain Big Data ersetzten könnte.

2 Hauptteil

2.1 Grundlagen

2.1.1 Big Data

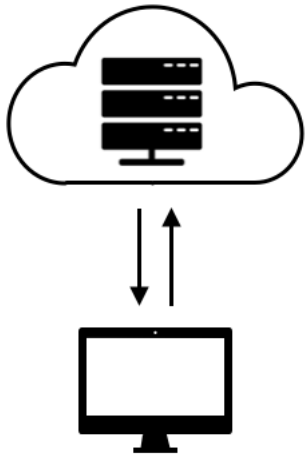
Es gibt keine exakte Definition für Big Data.[2, Seite 13] Diese Bezeichnung wird aber oftmals als Sammelbegriff benutzt für Daten, welche die Verarbeitungskapazität herkömmlicher Datenbanksysteme übersteigen, sowie für zentralere Datenbanksysteme, in welchen dies oft zutrifft. Im Laufe dieser Arbeit wird sich mit den Begriff Big Data auf das Web 2.0 bezogen. Doug Laney hat in einem Forschungsbericht Big Data an verschiedenen Variablen analysiert, die er auf die sog. „drei V“ zurückgeführt hat, nämlich volume, velocity and variety, also Umfang, Geschwindigkeit und Varianz. All diese Charakteristika können dazu führen, dass die Information nicht in die Datenbankstrukturen passt. Dennoch hat sich diese Form der zentralen Datenbanken durchgesetzt, so dass heutzutage fast alles, was digital ist, über eine Datenbank auf einem Server läuft. Big Data ist die Basis der heutigen Digitalisierung. Seit den 1960er Jahren gab es mehrere Weiterentwicklungen, welche das Sammeln, Speichern und Verwenden persönlicher Daten verbessert haben. So hat die Größe und der Umfang besagter Datenmenge exponentiell zugenommen, insbesondere durch stetig sinkende Speicherkosten, sowie durch zunehmend mächtigere Analysewerkzeuge. [2, Seite 190] Dennoch hat sich die den Datenbanken zugrundeliegende Technologie seit den 1960er Jahren kaum weiterentwickelt, weswegen unsere Daten lediglich durch Absicherung der Server geschützt sind.

2.1.1.1 Aufbau der Big Data

2.1.2 Big Data

Damit eine Website im Internet zugänglich ist, braucht ihr Inhalt einen eigenen Server. Um erreichbar zu sein, muss der Server jederzeit im Netz sein. Obwohl die meisten Website-Betreiber zu diesem Zweck die Datenzentren von Internet-Diensteanbietern nutzen, verfügen viele Unternehmen und Organisationen oft über eigene Webserver, um ihre Intranet- und Internet-Inhalte zu hosten. Der Webserver fungiert als Vermittler zwischen dem Inhalt der Webseite und dem Client, der sie empfängt. Wenn man eine Internetadresse in seinen Browser eingibt, sendet dieser eine Anfrage an den Nameserver, der aus dem Domänennamen die entsprechende IP-Adresse ermittelt. Der HTTP-Client des Browsers stellt dann über TCP (oder manchmal UDP) eine Verbindung zum Webserver her und sendet ihm eine Webseitenanforderung. Da komplette Webseiten aus verschiedenen HTML-Komponenten, Grafiken, Bildern und Videos bestehen, muss für jede Datei eine eigene Anfrage gestellt werden, auf die der Webserver mit dem Herunterladen des entsprechenden Inhalts antwortet. Der HTTP-Server sendet die angeforderten Dateien an den HTTP-Client, der sie mit Hilfe eines Interpreters auf dem Bildschirm anzeigt. Sobald der Client die komplette Webseite erhalten hat, wird die TCP-Verbindung wieder geschlossen. Die wohl bedeutendste Errungenschaft, welche den Umstieg zu Web 2.0 attraktiv machte, ist das sogenannte „Cloud Computing“.

Bild 1: Aufbau Big Data



Quelle: Token S. 19

Cloud Computing
Cloud Computing ist ein Modell für den bequemen Netzzugang auf Abruf zu einem gemeinsamen Pool konfigurierbarer Rechenressourcen (z. B. Datennetze, Server, Speichergeräte, Anwendungen und Dienste, entweder gemeinsam oder einzeln), die schnell bereitgestellt und mit minimalen Betriebskosten oder Rückgriff auf einen Anbieter freigegeben werden können. Cloud-Nutzer können die Kosten für die IT-Infrastruktur (kurz- und mittelfristig) erheblich senken und flexibel auf sich ändernde Anforderungen an die Datenverarbeitung reagieren, indem sie die elastischen Eigenschaften von Cloud-Diensten nutzen. Seit seiner Einführung im Jahr 2006 hat sich das Konzept in verschiedenen IT-Bereichen fest etabliert und gewinnt in der Praxis immer mehr an Boden: IDC schätzt, dass der Markt für öffentliches Cloud Computing im Jahr 2009 bereits 17 Mrd. USD wert war - etwa 5 Prozent des gesamten IT-Marktes, und im Jahr 2014 belaufen sich die Gesamtkosten von Unternehmen für Cloud Computing-bezogene Infrastrukturen und Dienste auf fast 175 Mrd. USD.

2.1.2.1 Beschreibung des Standes der Technik der Big Data

Nahezu jede Webseite oder anderweitige Anwendung mit Internetanschluss kommunizert heutzutage über einen zentralen Server. Dementsprechend ist mit Sicherheit zu sagen, dass die Technologie bereits existiert und stetig verbessert wird. Allerdings nur so weit, wie das Konzept von Big Data es erlaubt. So kann beispielsweise die Kommunikation zwischen Rechner und Server schneller gemacht oder auch die Sicherheit gesteigert werden, aber sie wird nie als ’unhackbar’ gelten.

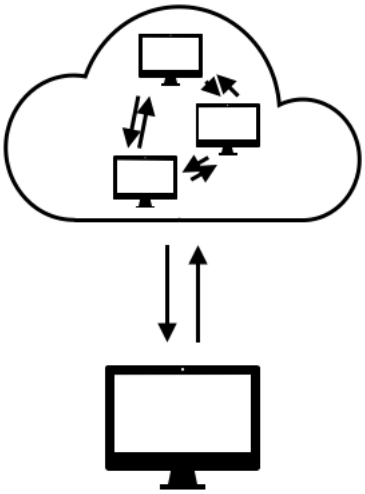
2.1.2.2 Anwendungsbeispiele

Wie bereits angemerkt gibt es heutzutage mehr Beispiele denn je für Applikationen mit Serveranbindung. Große Unternehmen wie Google und Meta haben Big Data einen ganz

neuen Namen verpasst, mit immensen Mengen an Daten, die durchgehend eingegeben und ausgegeben werden.

2.1.3 Blockchain

Bild 2: Aufbau Blockchain



Quelle: Token S. 19

Bei einer Blockchain handelt es sich um eine Kette von Transaktionen, die in den sogenannten Blöcken stattfinden. Blockchain-Software-Architekturen wurden ursprünglich entwickelt, um digitale Transaktionen sicherer zu machen. Die zugrundeliegende Technologie basiert auf den P2P Netzwerken. Jeder, der an einem Blockchain-Netz teilnehmen möchte, kann sich die Software herunterladen und sie auf seinem Rechner ausführen. Der Rechner wird damit zu einem neuen Knoten (Node) im Netz. Dadurch wird die ohnehin schon enorme Sicherheit noch einmal erhöht. Alle Transaktionen, die seit der Erstellung des ersten Knoten (auch als „Genesis Block“ bekannt) durchgeführt wurden, sind als verbundene Blöcke in einer verschlüsselten Datei gespeichert. Diese Datei existiert als Kopie auf jedem Knoten des Netzwerks. Mit der Blockchain wurde eine neue Technologie entwickelt, die es uns erstmals ermöglicht, der Datenbank im Kern zu vertrauen. Wie wir Daten speichern, verschlüsseln und fälschungssicher machen, wurde von Grund auf neu gedacht.

Token
Kryptografische Token stellen programmierbare Vermögens- oder Zugriffsrechte dar, die von einem intelligenten Vertrag und einem zugrundeliegenden verteilten Ledger verwaltet werden. Sie sind nur für die Person zugänglich, die den privaten Schlüssel für diese Adresse besitzt, und können nur mit diesem privaten Schlüssel signiert werden. Token könnten die Finanzwelt auf die gleiche Weise beeinflussen wie die E-Mail das Postsystem.

Hash
Umwandlung einer digitalen Datei unterschiedlicher Länge in eine Zeichenkette spezifischer Länge - im Secure Hashing Algorithm (SHA-256, der in der Kryptografie der Bitcoin-Blockchain benutzt wird) ist die Ausgabe immer 32 Bytes (256 Bits). Hashes sind

ungeheuer schwer umzukehren. Kenntnis des Hashs vermittelt keine Kenntnis der Datei, aber Kenntnis der Datei lässt sich ohne Weiteres in den Hash umwandeln. Jede noch so kleine Modifizierung der Datei verändert auf drastische Weise das Hashergebnis. Hashes decken daher jede Manipulation mit den gehashten Daten auf. [1, Seite 322]

Smart Contracts
Intelligente Verträge sind einfach auf einer Blockchain gespeicherte Programme, die ausgeführt werden, wenn bestimmte Bedingungen erfüllt sind. Sie werden häufig eingesetzt, um die rechtliche Abwicklung eines Vertrages zu automatisieren, so dass alle Parteien sofortige Gewissheit über das Ergebnis haben, ohne dass ein Vermittler eingeschaltet werden muss oder Zeit verloren geht. Sie können auch einen Arbeitsablauf automatisieren und die nächste Aktion auslösen, wenn die Bedingungen erfüllt sind.

2.1.3.1 Aufbau der Blockchain

Wie bereits erwähnt, setzt sich ein Blockchain-System aus mehreren Nodes zusammen. Im Folgenden soll nun die Struktur anhand der Teilsegmente dieses Systems in hierarchischer Ordnung erklärt werden.

Peer-to-Peer Netzwerke
Peer-to-Peer Verbindungen (kurz P2P) sind Netzwerke zwischen einzelnen Rechnern. Grundidee hinter P2P ist, dass Computer direkt Daten austauschen können, ohne dabei Umwege über Internetserver zu gehen.

Torrent Netzwerke
In einem Torrent-Netzwerk, wie beispielsweise BitTorrent, sind die Dateien nicht auf einem Server gespeichert, sondern sie werden in Teilsegmente unterteilt und auf mehreren Rechnern verteilt. Möchte man eine Datei aus solch einem Netzwerk herunterladen, dann müssen sämtliche Teile aus den verschiedenen Rechnern abgerufen werden. Durch diese Bündelung vieler Rechner erreicht man hohe Downloadgeschwindigkeiten, ohne zentrale Server betreiben zu müssen. Genau dieses Modell wäre ein P2P-Netzwerk.

Distributed Ledger
Distributed Ledger ist ein Oberbegriff für verschiedene Datenbanktechnologien, welche ein System zur dezentralen Speicherung von Daten wie beispielsweise Blockchain haben. Anders als bei einer zentralen Datenbank, gibt es hier keinen zentralen Administrator. Zur Kommunikation zwischen den einzelnen dezentralen Rechnern wird ein P2P-Netz eingesetzt. Ein Torrent-Netzwerk wäre ein Beispiel dazu.

Private Keys
Bei Distributed Ledger Systemen wird es im Allgemeinen zwischen zwei verschiedenen Arten unterschieden: Symmetrischer und asymmetrischer Verschlüsselung. Während bei einer symmetrischen Verschlüsselung ein und derselbe Schlüssel für die Ver- und Entschlüsselung der Daten erforderlich ist, gibt es bei der asymmetrischen zwei verschiedene. Letzteres wird bei der Blockchain verwendet. Bei den asymmetrischen Verschlüsselungen, wie z. B. Blockchain, funktioniert dies mithilfe von sogenannten Public und Privat Keys, welche mathematisch verlinkt sind: So kann man aus dem Private Key den Public

Key ermitteln, aber nicht andersherum. Mit dem Public Key eines Nutzers kann man eine Nachricht so verschlüsseln, dass sie nur mithilfe des passenden Private Keys lesbar wird. Dementsprechend ähnelt der Public Key sehr einer E-Mail-Adresse, an welche man Nachrichten senden, aber nur mithilfe eines Passwortes - in diesem Falle Private Key - lesen kann. Diese werden üblicherweise in einer Geldbörse gespeichert. Die Form dieser Wallet variiert zwischen einem Gerät, einem physischer Datenträger, einem Programm oder einem Dienst.

Wallet
Eine Blockchain-Wallet dient lediglich als sicherer Speicher des kryptografischen Schlüssels. Wallets speichern keine Tokens. Tokens stellen lediglich einen Eintrag im Ledger dar und werden vom Blockchain-Netzwerk gemeinschaftlich verwaltet. [4, Seite 88]

2.1.3.2 Beschreibung des Standes der Technik der Blockchain

Die erste Idee einer Blockchain wurde bereits 1991 beschrieben, und zwar in Form einer Lösung zum Zeitstempeln digitaler Dokumente, um sie rückwirkend vor Manipulation zu schützen. Diese Technologie wurde jedoch nie eingesetzt und das Patent erlosch 2004, vier Jahre vor dem Durchbruch der Blockchain-Technologie als Bitcoin-Netzwerk. Seitdem hat sich diese Branche ungemein entwickelt. Dezentrale Anwendungen werden in einem P2P-Netzwerk von Computern ausgeführt, anstatt auf einem einzelnen Computer. Es handelt sich dabei um ein Softwareprogramm, das so konzipiert ist, dass es nicht von einem einzigen Rechner kontrolliert wird. Dezentrale Anwendungen sind aber kein neues Phänomen und müssen nicht unbedingt auf einem Blockchain-Netzwerk laufen. Herkömmliche Webanwendungen verwenden beispielsweise HTML, CSS und JavaScript, um eine Webseite zu erstellen. Diese Seite interagiert mit einem Webserver, auf dem alle Daten gespeichert sind. Wenn man einen Dienst wie beispielsweise Twitter, Facebook, Amazon oder Airbnb nutzt, ruft die Webseite eine API auf, um seine persönliche Daten und andere notwendige Informationen, die auf seinen Servern gespeichert sind, zu verarbeiten und auf der aufgerufenen Seite anzuzeigen. Dezentrale Anwendungen sind traditionellen Webanwendungen ähnlich. Die Benutzeroberfläche einer dezentralen Anwendung entspricht einer Website oder einer mobilen App. Die Dateien dieser Benutzeroberflächen, wie Fotos, Videos oder Audiodateien, können auf dezentralen Speichernetzwerken wie Swarm oder IPFS gehostet werden. Derzeit werden sie aber oftmals noch zentral gehostet. Der Blockchain-Client verwendet die gleiche Technologie zum Erstellen einer Seite wie eine herkömmliche Webanwendung (z. B. HTML, CSS, JavaScript), nur dass die Informationen nicht von einem zentralen Server kommen, sondern von dem Blockchain-Client bzw. dem Blockchain-Netzwerk. Der Blockchain-Client bedient sowohl das Frontend als auch die P2P-Logik, die Wallet und gegebenenfalls die Smart Contracts (bei Smart-Contract-fähigen Netzwerken). Der Smart Contract interagiert mit einem Blockchain-Netzwerk, repräsentiert die Logik der dezentralen Anwendung und verarbeitet die Informationen aus Blockchain-Netzwerken und der Außenwelt, um den Zustand aller Netzwerkakteure zu verwalten (siehe Kapitel „Smart Contracts“). Repräsentiert der Blockchain-Client einen Full Node, verwaltet er auch den kompletten Ledger. In diesem Fall ist der Blockchain-Client HTTP-Client und -Server in einem, da bei einem Full Node alle Daten direkt beim Client liegen. Alles in allem ist diese Technologie nicht nur bereits vorhanden, sondern sie wird bereits genutzt und bietet den Nutzern große Vorteile. Die bekannteste Nutzung davon wäre die Struktur von Bitcoin bzw. von ähnlichen Online-Währungen. Es gibt jedoch auch viele andere Verwendungsmöglichkeiten, zum Beispiel

Bitcoin, Steemit und andere Anwendungen, auf die wir im Folgenden näher eingehen werden.

2.1.3.3 Anwendungsbeispiele

Bitcoin
Bitcoin ist eine dezentralisierte digitale Währung, die im Januar 2009 geschaffen wurde. Sie folgt den Ideen, die in einem White Paper des mysteriösen und pseudonymen Satoshi Nakamoto dargelegt wurden. Die Identität der Person oder Personen, die die Technologie entwickelt haben, bleibt ein Geheimnis. Bitcoin verspricht niedrigere Transaktionsgebühren als herkömmliche Online-Zahlungsmechanismen und wird im Gegensatz zu staatlich ausgegebenen Währungen von einer dezentralen Behörde verwaltet. Bitcoin ist als eine Art Kryptowährung bekannt, weil sie Kryptographie verwendet, um ihre Sicherheit zu gewährleisten. Es gibt keine physischen Bitcoins, sondern Guthaben in einem öffentlichen Hauptbuch, auf das jeder zugreifen kann (obwohl alle Aufzeichnungen verschlüsselt sind). Alle Bitcoin-Transaktionen werden durch eine enorme Menge an Rechenleistung in einem Prozess verifiziert, der als Mining bekannt ist. Obwohl Bitcoin in den meisten Teilen der Welt kein gesetzliches Zahlungsmittel ist, erfreut er sich großer Beliebtheit und hat die Einführung von Hunderten anderer Kryptowährungen, den sogenannten Altcoins, ausgelöst. Bitcoin wird im Handel oft als BTC abgekürzt.

Steemit
Steemit ist eine Blockchain-basierte Social-Media-App, die Gemeinschaften schafft, in denen die Nutzer fürs Teilen ihrer Stimme belohnt werden. Es ist eine neue Art Aufmerksamkeitsökonomie. Hier sind Nutzer in der Lage, Tokens zu gewinnen, sogenannte STEEM's, welche gegen herkömmliche Währungen umgetauscht werden können. Im Grunde gibt es vier verschiedene Möglichkeiten, diese zu erhalten: Inhalte posten, Freiberufliche Tätigkeit, Teilnahme an Wettbewerben und Herausforderungen oder das Handeln mit dem STEEM Token.

Brave Browser
Das Ziel dieses Browsers ist es, den Nutzern die Kontrolle darüber zu geben, welche Werbung sie sehen, und letztendlich jede Werbung von Drittanbietern zu entfernen, die als aufdringlich angesehen werden könnte. Außerdem sollen Tracker von Drittanbietern entfernt werden. Um den Nutzern die Kontrolle darüber zu geben, welche Werbung sie sehen, verifiziert der Browser, welche Werbung dann individuell auf dem Browser platziert werden soll. Die Nutzer können sich dann dafür entscheiden, diese zu sehen, wenn sie das möchten. Die Nutzer können dann in einer Kryptowährung fürs Ansehen von Werbung verifizierter Verlage bezahlt werden. Bei der Währung handelt es sich um ein auf Blockchain basierendes Token, das sogenannte Basic Attention Token (kurz BAT). Da Brave Werbung von Drittanbietern blockiert, muss der Browser weniger Inhalte herunterladen, wenn Nutzer im Internet surfen, was bedeutet, dass die Ladezeiten schneller sind als bei vielen anderen gängigen Browsern.

2.2 Erkenntnisse

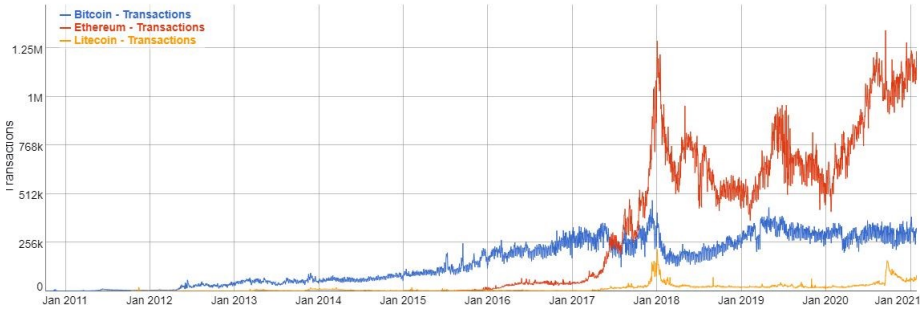
2.2.1 Literaturanalyse

2.2.2 Diskussion der Forschungsfrage

Im Darauffolgenden soll ein näherer Blick auf den bisherigen Blockchaintrend geworfen werden und danach sollen beide Netzwerktypen auf verschiedene Aspekte gegeneinander gestellt werden, um die Möglichkeit abzuwägen, ob die Blockchain-Technologie in Zukunft das gegenwärtige System ersetzten wird.

In den letzten Jahren hat Blockchain an großer Bedeutung gewonnen.

Bild 3: Trend von Kryptowährungen



Quelle: Token S. 24

Ist der Trend begründet und wird sich die Technologie durchsetzten?

„This is an important time in the blockchain market as enterprises across markets and industries continue to increase their investment in the technology. The pandemic highlighted the need for more resilient, more transparent supply chains, healthcare delivery, financial services, and so much more, and enterprises around the world have been investing in blockchain to provide that resiliency and transparency, What is also very important right now is that we are seeing real interest and investment by corporations, financial institutions, and even governments in areas they previously viewed with some uncertainty such as cryptocurrencies, digital assets, central bank digital currencies, decentralized finance, and stablecoins. This investment will have major implications in a very short time on everything from retail to financial services to capital markets.“ [10]

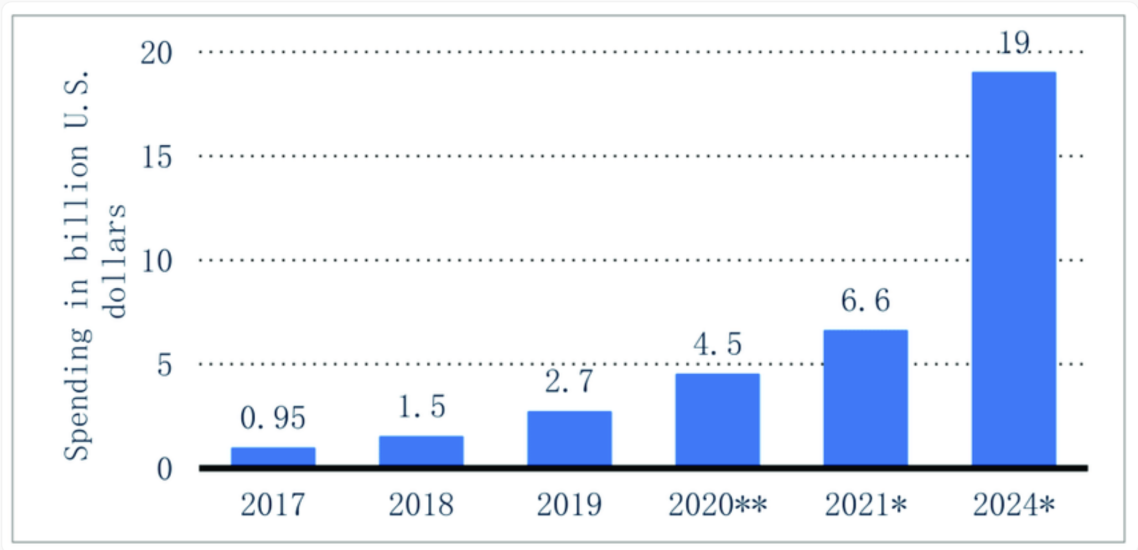
Dieses Zitat stammt von James Wester, Forschungsdirektor von Worldwide Blockschain Solutions. Laut ihm besteht kein Zweifel, dass Blockchainsysteme weiterhin wachsen und sich weiter entwickeln werden. Belegt wird dieses Argument durch die jährlich steigenden Investitionen in Blockchain Solutions (siehe Abbildung unten).

Im Folgenden sollen nun beide Datenbanksysteme auf deren Wichtigste Kriterien untersucht werden.

Kontrolle für Unternehmen

Unternehmen benötigen einen bestimmten autoritativen Prozess, um die Blockchain-Technologie zu nutzen. Anders als Big Data Anwendungen, werden öffentliche Blockchains nicht in der Lage sein, diese Kontrollmöglichkeiten in absehbarer Zeit zu bieten.

Bild 4: Trend von Kryptowährungen



Quelle:
https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/

Der Aufstieg privater und konzerninterner Blockchains scheint jedoch sowohl die Kontrolle als auch den dezentralen Charakter der Technologie zu bieten. Diese werden meist als Enterprise-Blockchain-Frameworks bezeichnet und sind nur für Organisationen geeignet.

Sicherheit
„Sicherheit ist kein Vorteil oder Upgrade. Man erreicht sie nicht, indem man neue Schichten aus Passwörtern hinzufügt.“ [1, Seite 22] Durch ihre grundlegende Funktionsweise, Transaktionen und Daten auf vielen Rechnern eines Systems zu verteilen, hat die Verschlüsselung bei Blockchains einen hohen Stellenwert. So würde beispielsweise der Angriff auf ein Bitcoin rund 30 Mrd. USD kosten.[9] Dies geschieht durch Umschreibung der Information in eine anscheinend zufällige Abfolge von Zeichen. Dies geschieht durch den sogenannten Schlüssel, welcher erforderlich ist, um die Information zu decodieren. Anders als bei der Blockchain, vertritt Big Data den umgekehrten Ansatz. Die Idee hinter Big Data ist, dass die frühere langsame, unbeholfene, schrittweise vorgehende Suche nach Wissen durch menschliche Gehirne ersetzt werden kann, wenn zwei Bedingungen zutreffen: Alle Daten in der Welt können an einem einzigen Ort gesammelt werden und es können Algorithmen geschrieben werden, die hinreichend umfangreich sind, um sie zu analysieren.[1, Seite 35] Hier besteht oftmals die Gefahr, dass, sollte besagter Server offline gehen oder sogar kompromitiert werden, die Web-Applikation nicht zuverlässig ist.

Fälschungssicher
Ein Versuch, einen Block in der Blockchain zu manipulieren, würde den Hashwert dieses Blockes ändern, da sich der Inhalt ändert. [3, Seite 100] Der sogenannte Konsensmechanismus ist ein Programm, das die einzelnen Knotenpunkte innerhalb einer Blockchain vergleicht und in der Lage ist, legitime Transaktionen erst zu identifizieren und dann der Blockchain hinzuzufügen. Grund hierfür ist die Tatsache, dass jeder einen Block zur Blockchain hinzufügen kann, weswegen sichergestellt werden muss, dass keine falschen

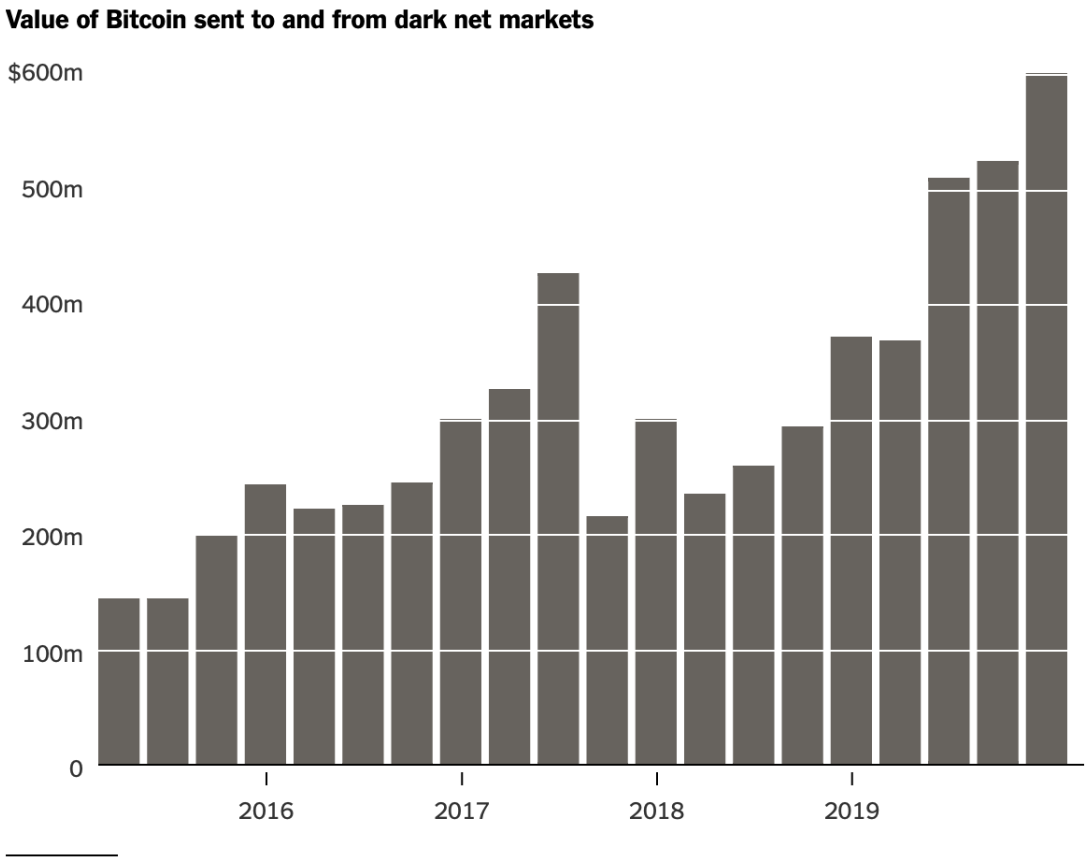
Informationen zu Elementen der Blockchain werden. Des Weiteren sorgt er dafür, dass es eine allgemeine Übereinkunft der Daten innerhalb des Blockchain-Netzwerkes gibt, so dass die Verlässlichkeit dieser Daten gewährleistet wird.

Kontrolle
Wie bereits in der Einleitung erwähnt, war einer der ausschlaggebendsten Elemente der Web 2.0-Epoche, dass die Nutzer auch die Rolle eines Produktes übernehmen. Das zeigt sich beispielsweise an der Sammlung von Nutzerinformationen, welche dann genutzt werden, um für jeden Nutzer spezifische Werbungen zu schicken, je nach seinen Vorlieben. Dies soll im Web 3.0 mit Hilfe von Blockchain von Grund auf anders aufgebaut werden. Stichwort Basic Attention Token, kurz BAT. BAT ist ein System, welches in der Lage ist, die Aufmerksamkeit der Nutzer direkt zu belohnen. Somit wird die Rolle aller Akteure der Onlinewerbebranche neu definiert, wie auch die Beziehung zwischen Nutzern, Publicer und Werbetreibenden. Ziel dieser Idee ist, einen transparenteren und effizienteren Werbemarkt zu schaffen. BAT ist ein Token, welches von einer Public Blockchain verwaltet wird. Der Brave Browser hat eine integrierte Wallet, die zwei Tokens verwaltet: BAT, welches als Zahlungsmittel verwendet wird, und Basic Attention Metrics, das sicherstellt, dass die Aufmerksamkeit der Nutzer genau gemessen und berichtet wird. Werbetreibende senden diese BAT Tokens mitsamt den Werbeanzeigen verschlüsselt per Smart Contract. Sollte sich ein Nutzer dazu entscheiden, die Werbung anzusehen, kann er bis zu 70 Prozent der Werbeeinnahmen verdienen. Der Rest geht an den Webseitenbetreiber.

Anonymität
Bei Web 2.0 Anwendungen findet die Nutzererkennung anhand der E-Mail-Adresse oder Benutzernamens zusätzlich des Passwortes statt. Diese Informationen sind auf einem Server hinterlegt und werden geprüft, beispielsweise bei der Anmeldung. Bei der Blockchain hingegen findet dies durch den Private Key statt, welcher auf einem P2P verschlüsselt hinterlegt ist. Durch die hohe Verschlüsselung, sowie durch die hinter Private Keys versteckte Anonymität gelten Blockchain Datenbanksysteme als Möglichkeit, unbekannt im Netz zu agieren. Dies hat sich bereits als reale Gefahr dargestellt, da viele illegale Aktivitäten, insbesondere im Zahlungsverfahren heutzutage über Kryptowährungen, wie typischerweise Bitcoin, ablaufen. Insbesondere weil diese Zahlungen nicht nachverfolgbar sind. *„Der Betrag an Kryptowährung, der auf dem sogenannten Dark-Web-Marktplatz ausgegeben wurde, stieg in den letzten drei Monaten des Jahres 2019 um 60 Prozent auf einen neuen Höchststand von 601 Millionen US-Dollar, wie aus den am Dienstag veröffentlichten Daten von Chainalysis hervorgeht, einem Unternehmen, das alle Bitcoin-Transaktionen verfolgt und als Berater für mehrere Regierungsbehörden fungiert.* [8]

Energieverbrauch
Bei Big Data Netzwerken setzt sich der Energieverbrauch aus der durchgehenden Stromzufuhr des Servers und der des Kühlsystems zusammen, was zu hohen Energiekosten für das Unternehmen führt. Bestimmte Blockchain-Konsensmechanismen haben jedoch höhere Energiekosten. Wie bereits angemerkt muss ein Konsensprozess durchgeführt werden, um sicherzustellen, dass jede Transaktion gültig ist. Es liegt auf der Hand, dass der Konsensprozess einen enormen Aufwand für die Bildung jedes Knotens erfordert. Ganz zu schweigen davon, dass alle Knoten hin und her kommunizieren müssen, um

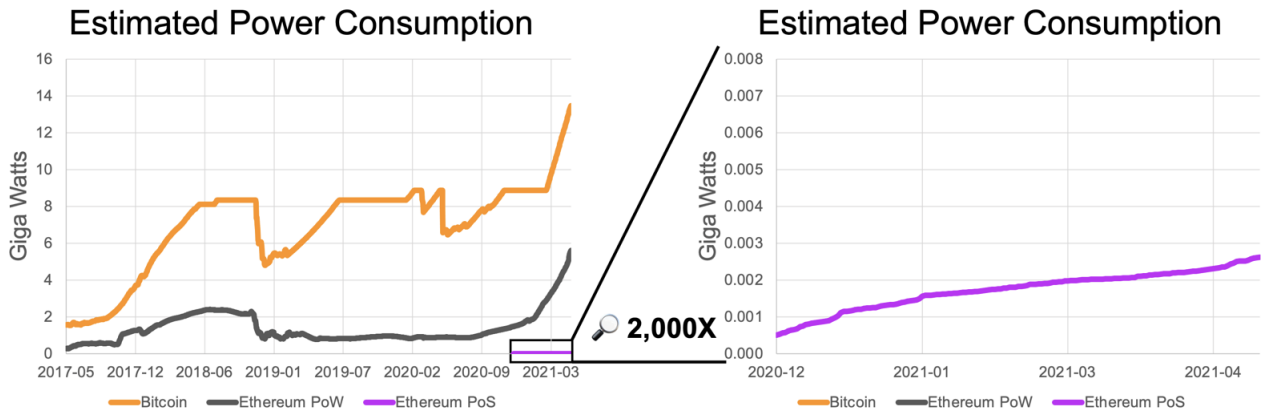
Bild 5: Bitcoin Wert im Darknet



Quelle: Token S. 19

sicherzustellen, dass eine Transaktion gültig ist. Einige Blockchain-Netzwerke, wie beispielsweise Bitcoin, verwenden hierbei den Proof of Work, bei welchem jeder Node eine mathematische Funktion löst. Der erste, der die Lösung der Funktion findet, bekommt als Belohnung Bitcoins. Es gibt aber auch andere Konsensmechanismen, bei denen der Energieverbrauch deutlich geringer ist, so beispielsweise der Proof of Stake. Anders als bei den Proof of Work, wird bei dem Proof of Stake gelost. Der Gewinner, auch Validator genannt, überprüft den nächsten Block und alle darin aufgezeichneten Transaktionen. Um an diesem Losverfahren teilzunehmen, müssen die Knoten, die als Validator fungieren wollen, eine bestimmte Anzahl von Coins in das Netz einbringen, was im Grunde als Garantie fungiert. Je höher die Anzahl der Coins, der sogenannten Stake, desto höher ist die Wahrscheinlichkeit, als Validator ausgewählt zu werden. Die als Garantie hinterlegten Coins garantieren auch, dass der Prüfer keine betrügerischen Transaktionen akzeptiert: tut er dies doch, verliert er einen Teil seines Stakes. Als Belohnung für die Überprüfung erhält der Überprüfer in der Regel eine Transaktionsgebühr in Form eines Tokens des jeweiligen Netzwerkes.

Bild 6: Energieverbrauch PoW vs PoS



Quelle: Token S. 19

Kosten
Zusätzlich zu den Energiekosten fallen noch weitere Gebühren an wie Hardware, Infrastruktur und Personal. Bei einem dezentralen Netzwerk werden diese Dienstleistungen outsourced auf Freiwilligenbasis der Nutzer.

2.2.3 Gründe für die Wahl der Hypothese

Wie aus dem vorherigen Kapitel zu entnehmen ist, bieten sowohl Big Data als auch Blockchainsysteme viele verschiedene Vor- und Nachteile für Internetdienstleister. Dezentrale Systeme haben die letzten Jahrzehnte stark geprägt und den Weg für viele neue Ideen und Systeme eröffnet. Es gibt immer mehr Skandale in punkto Datenraub oder Intransparenz zentraler Webseitenbetreiber, was die allgemeine Nachfrage nach neuen, sichereren Alternativen steigen lässt. Zusammen mit der sich verbessernden Technologien und den oben genannten Vorteilen lohnt es sich für viele Unternehmen, schon heute auf Blockchain umzusteigen. Selbst wenn es ein eher langwieriger Prozess wird, wären vermutlich zehn Jahre ein denkbares Zeitfenster, um besagtes Ziel zu erreichen.

2.2.4 Diskussion

2.2.4.1 Umsetzbarkeit

Da die zugrundeliegende Technologie dafür schon gegeben ist, wäre die Frage vielmehr, ob sich die Umstellung für Unternehmen langfristig lohnt. BitTorrent, Popcorn Time, BitMessage und Tor sind allesamt dezentrale Anwendungen, die von einem PHP-Netzwerk verwaltet werden, das kein Blockchain-Netzwerk ist. Blockchain-Netzwerke sind eine verbesserte Form von P2P-Netzwerken.

Public/Private Blockchain
Der Unterschied zwischen einer Public und einer Private Blockchain liegt darin, wer Mitglied des Netzwerks sein und die Konsensmechanismen ausführen darf. Jeder, der die im Protokoll festgelegten Regeln und Verfahren befolgt, kann einem öffentlichen Blockchain-

Netzwerk beitreten. Bitcoin zum Beispiel ist ein öffentliches Blockchain-Netzwerk. Im Gegensatz dazu ist ein privates Blockchain-Netzwerk geschlossen. Private Netzwerke können nur per Einladung beigetreten werden. Mitglieder müssen nach bestimmten Regeln validiert werden. Hier wird bestimmt, wer was sehen kann und wer an welchen Transaktionen teilnehmen darf. Private Blockchains werden in der Regel von Unternehmen oder Regierungen betrieben, dabei können sich u. U. Einzelpersonen oder Organisationen daran beteiligen.

Da außerdem die meisten Unternehmen bereits über ein zentrales Datenbanksystem verfügen, müssten sie für die entstehenden Kosten eines Wechsels aufkommen. Man beachte hierbei, dass es aufgrund der Tatsache, dass die dazu erforderliche Technologie ein relativ wenig verbreitetes Konzept ist, nicht viele fähige Entwickler gibt, die daran arbeiten können. Wenn Unternehmen also versuchen, ihre Blockchain-Lösung für den eigenen Betrieb zu entwickeln, kann es u. U. schwierig werden, ein fähiges Team fürs Projekt zu finden. Blockchain ist nicht für Unternehmen gedacht, die Legacy-Netzwerke (ältere Systeme) betreiben. In Wirklichkeit würde die Blockchain die alten Netze ersetzen. Allerdings ist der Integrationsprozess noch nicht voll funktionsfähig. Außerdem sind viele Blockchain-Technologien nicht in der Lage, mit den alten Netzen zusammenzuarbeiten. Das bedeutet, dass die Unternehmen, um sie richtig nutzen zu können, ihre alten Netze endgültig abschaffen müssten. Diesem Umstand stehen viele skeptisch gegenüber.

2.2.4.2 Zukunftstauglichkeit

Das Internet hat sich in den letzten Jahren zu einem Einkaufsladen für Benutzerinformationen verwandelt, von welchem die Nutzer kaum profitieren. P2P-Netzwerke wie Blockchain versprechen hier Anonymität, Kontrolle und Sicherheit und vor allem weniger Abhängigkeit von Unternehmen.

„Wir überschätzen immer die Veränderungen, die in den nächsten beiden Jahren passieren sollen. Aber wir unterschätzen den Wandel, der über die nächsten zehn Jahre passiert. Lass dich dadurch nicht zur Untätigkeit verleiten.“ - Bill Gates [3, Seite 46]

Wie bereits festgestellt existiert bereits eine vielversprechende Technologie dazu. Im letzten Jahrzehnt kam es zu hunderten Skandalen von Big-Data-Unternehmen aufgrund ihrer teilweise fragwürdigen Strategien, Profit zu erzielen. Auf Blockchain basierende Seiten bieten hingegen eine höhere Transparenz, sowie die Möglichkeit für Nutzer, sich an diesem Prozess finanziell selbst zu bereichern. Auch wenn die Technologie von Blockchain Netzwerken und der gesetzliche Rahmen dazu noch nicht ausgereift ist, besagt der Trend, dass wir damit zu rechnen haben, zumal es bereits funktionierende Geschäftsmodelle und Währungen gibt. Viele Tech-Führungskräfte und Ingenieure haben bereits große IT-Unternehmen wie Google, Meta und Amazon verlassen, um die ihrer Meinung nach einmalige Chance der Kryptowährung zu nutzen.[7]

2.2.5 Fazit

Auch wenn wir uns mittlerweile auf die Zuverlässigkeit unzähliger Dienste verlassen, laufen im Hintergrund Datenbanken, welche im Kern wenig Sicherheit gewährleisten können. Unberechtigte Zugriffe sind möglich und können nicht immer verfolgt werden. DLTs ändern das, und so sind sie denkbar eine Technologie fürs kommende Zeitalter. Verschlüsselung, Speicherung, Validierung und Sicherung der Daten funktionieren hier in einer integrierten Lösung. Alle Daten, denen wir vertrauen müssen, werden in Zukunft

in einem Distributed Ledger bzw. einer Blockchain gespeichert werden. Neue Geschäftsmodelle können entstehen – direkt zwischen Nutzern und Anbietern, ohne Mittelsmänner. Es ist allerdings auch zu bedenken, dass herkömmliche Datenbanken deutlich effizienter, einfacher und günstiger zu betreiben sind. Überall dort, wo wir die Sicherheit der Blockchain oder Funktionen wie Smart Contracts nicht brauchen, sind sie daher weiterhin die bessere Wahl.

2.2.6 Verifikation der Hypothese

Bei der Überprüfung dieser These, ist festzustellen, dass auch wenn der genaue Zeitramen ungewiss ist, so scheint der allgemeine Trend, sowie die vielversprechenden Vorteile, welche die Blockchain Struktur zu bieten haben, darauf hinzudeuten, dass mit an sicherheit grenzender Wahrscheinlichkeit sich diese bewahrheiten wird.

3 Schluss

3.1 Kurzzusammenfassung der Arbeit

Zusammenfassend lässt sich sagen, dass Blockchain die gleichen Grundbausteine bietet wie die, welche für Big Data Netzwerke benutzt werden. Allerding bildet seine einzigartige Strukur die Basis für viele neue Optionen sowie Innovationen. Darüber hinaus ist das gesamte Konzept dieses Datenbanksystems darauf ausgerichtet, den Nutzer eine höhere Menge an Sicherheit, Anonymität und Kontrolle anzubieten. Alles in allem hat das bereits in den letzten Jahren zu einer stetig steigenden Nachfrage nach auf Blockchain basierenden Netzwerken geführt. Im Laufe dieser Arbeit wurde gezeigt, dass anzunehmen ist, dass dieser Trend exponentiell weitersteigen wird.

3.2 Ausblick

Spannend wird es zu sehen, was die Weiterentwicklung von Quantencomputern für Hashes und Kryptografie und folglich auch für DLTs bedeuten wird. Aber bis es so weit ist, ist die Blockchain die mit Abstand sicherste Form der Transaktionsdokumentation

Literaturverzeichnis

[1] Georg Gilder: *Das Leben nach Google. Der Absturz von Big Data und der Aufstieg der Blockchain*. Plassen: Kulmbach. 2018.

[2] Viktor Mayer-Schöneberger, Kenneth Cukier: *Big Data. Die Revolution, die unser Leben verändern wird*. Redline: München. 2017.

[3] Frank Thelen: *10xDna*. Goldmann: Leipzig. 2021.

[4] Shermin Voshmgir: *Token Economy. Wie das Web3 das Internet revolutioniert*. Token Kitchen: Luxemburg. 2020.

[5] Douglas Adams: *Hyperland* (1990) `https://www.youtube.com/watch?v=1iAJPoc23-M&t=17s` Bearbeitungsstand: 23.05.2014, [Zugriff 2022-01-01]

[6] *Web 2.0* `https://de.wikipedia.org/wiki/Web_2.0` Bearbeitungsstand: 03.01.2014, [Zugriff 2022-01-01]

[7] Daisuke Wakabayashi, Mike Isaac: *The New Get-Rich-Faster Job in Silicon Valley: Crypto Start-Ups* (20.12.2021) `https://www.nytimes.com/2021/12/20/technology/silicon-valley-cryptocurrency-start-ups.html?searchResultPosition=4` Bearbeitungsstand: 22.12.2021, [Zugriff 2022-01-01]

[8] Nathaniel Popper: *Bitcoin Has Lost Steam. But Criminals Still Love It.* `https://www.nytimes.com/2020/01/28/technology/bitcoin-black-market.html` Bearbeitungsstand: 28.01.2020, [Zugriff 2022-01-01]

[9] *Cost of a Bitcoin Attack* `https://gobitcoin.io/tools/cost-51-attack/` Bearbeitungsstand: 01.01.2022, [Zugriff 2022-01-01]

[10] *Global Spending on Blockchain Solutions Forecast* `https://www.idc.com/getdoc.jsp?containerId=prUS47617821` Bearbeitungsstand: 19.04.2021, [Zugriff 2022-01-01]

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbstständig und ohne unerlaubte Hilfe angefertigt worden ist, insbesondere dass ich alle Stellen, die wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen sind, durch Zitate als solche gekennzeichnet habe. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Weiterhin erkläre ich, dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde/Prüfungsstelle vorgelegen hat. Ich er- kläre mich damit einverstanden, dass die Arbeit der Öffentlichkeit zugänglich gemacht wird. Ich erkläre mich damit einverstanden, dass die Digitalversion dieser Arbeit zwecks Plagiatsprüfung auf die Server externer Anbieter hochgeladen werden darf. Die Plagiatsprüfung stellt keine Zurverfügungstellung für die Öffentlichkeit dar.

München, den 10. Januar 2022

Leonardo Ciria Buil

Abstract

Im Laufe der Zeit hat sich das Internet über verschiedene sogenannte Epochen entwickelt, welche sich stark voneinander unterscheiden. Wir befinden uns gegenwärtig in der Web2-Ära, aber schon mit einigen Web3-Elementen. Ziel dieser Arbeit ist es herauszufinden, ob und wann die Web3-Epoche, welche insbesondere von Blockchain-Strukturen und ähnlichen P2P-Netzwerken geprägt ist, die gegenwärtige ersetzen wird. Im Verlauf dieser Arbeit wird ein genauerer Blick auf den Blockchain-Trend geworfen, verschiedene Vor- und Nachteile beider Strukturen werden abgewägt. Hierei handelt es sich um:

- Kontrolle für Unternehmen
- Sicherheit
- Fälschungssicher
- Anonymität
- Energieverbrauch
- Kosten

Anschließend wird die Logik hinter der Umsetzung und die Zukunftstauglichkeit näher angeschaut. Im Verlaufe dieser Arbeit kommt der Autor zum Schluss, dass die Umsetzung auf Blockchain-basierende Datenbanksysteme sehr wahrscheinlich ist, ja es ist zu erwarten, dass bereits in den nächsten Jahren Blockchain-Netzwerke einen zunehmenden Anteil sämtlicher Datenbanksysteme abdecken wird.