



AALBORG UNIVERSITY
DENMARK

Aalborg Universitet

Blockchains, Smart Contracts, und das Dezentrale Web

Voshmgir, Shermin; Technologiestiftung Berlin

Creative Commons License
CC BY-SA 4.0

Publication date:
2016

Document Version
Også kaldet Forlagets PDF

[Link to publication from Aalborg University](#)

Citation for published version (APA):

Voshmgir, S., & Technologiestiftung Berlin (2016). *Blockchains, Smart Contracts, und das Dezentrale Web*. Technologiestiftung Berlin.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- ? Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- ? You may not further distribute the material or use it for any profit-making activity or commercial gain
- ? You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Eine Publikation der

**TECHNOLOGIE
STIFTUNG
BERLIN**

Blockchains, Smart Contracts und das Dezentrale Web

Shermin Voshmgir



Impressum

Technologiestiftung Berlin 2016
Fasanenstraße 85 · 10623 Berlin · Telefon +49 30 46302 400
info@technologiestiftung-berlin.de · technologiestiftung-berlin.de

Autorin

Dr. Shermin Voshmgir

Herausgeber

Dr. Christian Hammel

Gestaltung

Lippert Studios, Berlin

Druck

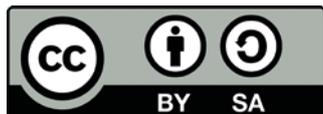
LM Druck und Medien GmbH, Freudenberg

Titelbild

Lippert Studios, Berlin



Dieses Projekt wird von der Senatsverwaltung für Wirtschaft, Technologie und Forschung und der Investitionsbank Berlin aus Mitteln des Landes Berlin gefördert.



Textinhalte, Tabellen und Abbildungen dieses Werkes, mit Ausnahme der Abbildungen 8 und 9, können genutzt und geteilt werden unter einer Creative Commons - Lizenz Namensnennung - Weitergabe unter gleichen Bedingungen 3.0 Deutschland (siehe <http://creativecommons.org/licenses/by-sa/3.0/de/>).

Als Namensnennung für Text und Tabellen ist anzugeben: Shermin Voshmgir, Blockchains, Smart Contracts und das Dezentrale Web, Technologiestiftung Berlin, 2016. Wo an Tabellen

und Abbildungen Quellen angegeben sind, sind diese ebenfalls als Quelle zu nennen.

Die Autorin weiß um die Bedeutung einer geschlechtergerechten Sprache und befürwortet grundsätzlich den Gebrauch von Parallelformulierungen. Von einer durchgehenden Benennung beider Geschlechter bzw. der konsequenten Verwendung geschlechterneutraler Bezeichnungen wurde im vorliegenden Text dennoch abgesehen, weil die Lesbarkeit deutlich erschwert würde.

Inhalt

Vorwort	5
Zusammenfassung	6
Executive Summary	7
1. Über Blockchain	8
1.1 Blockchain und die Entwicklung des Web	9
1.2 World Wide Web	10
1.3 Technologie hinter Blockchain	12
1.4 Wofür kann man die Blockchain verwenden?	14
1.5 Welche Blockchains gibt es?	15
1.6 Status Quo und langfristiges Potenzial	16
2. Branchen und Anwendungsgebiete	17
2.1 Banken, Versicherungen und FinTech	18
2.2 Sharing Economy, Internet of Things und Industrie 4.0	19
2.3 Sharing Economy und Kreativwirtschaft	20
2.4 Notare, Grundbücher und eGovernment	21
2.5 Buchhaltung, Buchprüfung und Auditing	22
2.6 Supply Chain	22
2.7 Gesundheitswesen	23
2.8 Energiewirtschaft	24
2.9 IT Dienstleistungen	26
2.10 Legal Tech und neue juristische Sachverhalte	26
2.11 Forschungsbedarf	27
3. Standort Berlin	28
3.1 Startups	28
3.2 Etablierte Firmen und Institutionen im Blockchain Umfeld	29
3.3 Forschung und Lehre	29
3.4 Meetups in Berlin	29
4. Potenziale und Herausforderungen	30
5. Handlungsempfehlungen für den Standort Berlin	31
5.1 Förderungen von Pilotprojekten	31
5.2 Rechtssicherheit schaffen	31
5.3 Information und Ausbildung	32
5.4 Kooperationsnetzwerke und Veranstaltungen	32
5.5 Förderungen der Basistechnologien und Blockchain Startups	33
Interviewpartner	34
Quellen und weiterführende Informationen	35

Blockchain-City Berlin

Kennen Sie Blockchain? Sie ist jedenfalls aus den Wirtschaftsnachrichten nicht mehr wegzudenken. Das Interesse an der Blockchain ist ungebrochen und nimmt laufend zu. Mittlerweile wird sogar von einer "Blockchain-Revolution" gesprochen, die unsere Welt verändern wird. Nüchtern betrachtet dürfte allerdings klar sein, dass hier auch ein gewisses Maß an Überschlag zu konstatieren ist.

Noch vor wenigen Monaten wurde die Blockchain vor allem mit Kryptowährungen wie Bitcoin in Verbindung gebracht. Doch es wird immer deutlicher, dass auch viele andere Bereiche von ihr profitieren können: Die Blockchain ist im Kern eine Alternative zu Zertifikaten, staatlichen Registern und öffentlichen Beglaubigungen. Sie basiert auf dem Gedanken, dass die Wahrheit und Richtigkeit ihrer Informationen durch die Vielzahl der öffentlichen Kopien ihrer selbst innerhalb der Online-Community sichergestellt ist.

Sie ist also vor allem dort stark, wo vorhandene Strukturen das Vertrauen in die Richtigkeit von Transaktionen und Informationen nicht gewährleisten können. Dies dürfte ein Grund dafür sein, dass die Blockchain beispielsweise als Alternative zu Grundbüchern vor allem in Ländern, deren Verwaltung

vor besonderen Herausforderungen steht, von besonderem Interesse ist. Aber sie kann auch, und das macht sie im wirtschaftlichen Kontext so attraktiv und disruptiv, als kostengünstigere Alternative zu komplexen Verfahren und Verträgen dabei helfen, Transaktionskosten erheblich zu senken.

Mit unserer Studie wollen wir nicht nur einen Überblick über die Technologie geben, sondern auch konkrete Anwendungsmöglichkeiten aufzeigen. Wir geben praktische Antworten auf die Fragen: Wer forscht und entwickelt in Berlin an Blockchains? Welche Berliner Anwender könnten die Technologie einsetzen? Zu welchen Zwecken? Wo stehen wir im überregionalen Vergleich?

Eines lässt sich bereits an dieser Stelle mit Sicherheit sagen: Berlin ist der wichtigste Standort für die Entwicklung von Blockchain-Technologien in Deutschland - wer die Chancen der Blockchain nutzen will, ist in Berlin richtig.

Nicolas Zimmer

Vorstandsvorsitzender
Technologiestiftung Berlin

Zusammenfassung

Blockchain ist eine neue Technologie der Verifizierung von Datentransaktionen. Es handelt sich um eine Form der Verteilung und Sicherung von Daten, auf deren Basis viele Funktionen zentral organisierter Informationssysteme dezentralisiert werden können. Die Blockchain kann überall dort zum Einsatz kommen, wo Informationen sicher verwaltet und verifiziert werden müssen und es normalerweise eines Vermittlers bedarf.

Die Blockchain baut unter anderem auf der Logik der Peer-to-Peer (P2P) Netzwerke auf und löst das Problem der zentralen Datenspeicherung und Transaktionsvalidierung. Sie kann damit ein nächster großer Schritt in der Entwicklung der Computer und des Internets sein. Was ist damit gemeint? Das WWW hat den Informationsaustausch revolutioniert. Das sogenannte Web2 machte das Web programmierbar und brachte uns Social Media und die Sharing Economy. Blockchain kann in dieser Entwicklungsreihe als ein Baustein des Web3 gesehen werden, der den Wertaustausch revolutioniert, indem er P2P-Transaktionen ohne zentrale Clearingstelle ermöglicht. Auf dieses Transaktionsprotokoll können Smart Contracts, dezentrale Anwendungen (dApps) und Dezentrale Autonome Organisationen (DAOs) aufbauen.

Die Studie identifiziert wesentliche Berliner Akteure und zeigt mögliche Handlungsmaßnahmen für Unternehmen, Wissenschaft und Politik auf. Mögliche Blockchain Anwendungen werden über eine ganze Reihe von Branchen hinweg vorgestellt: Banking und Fintech, Kreativwirtschaft, Sharing Economy, Energiesektor, eGovernment, Legal Tech, Gesundheit und (IT-) Consulting. Darüber hinaus werden aktuelle Forschungsfelder für die Wissenschaft aufgezeigt.

Die wichtigsten Erkenntnisse und Empfehlungen sind:

(1) Blockchain-Technologien sind eine Alternative zu Anwendungen, die auf zentralen Clearingstellen oder zentralen Vertrauensinstanzen beruhen. Sicherheit und Angreifbarkeit

unterscheiden sich dementsprechend wesentlich von herkömmlichen Anwendungen.

(2) Blockchain-Technologien haben Anwendungspotenziale in einer Vielzahl von Branchen. Sie ermöglichen neue Formen der Abwicklung von Geschäften, indem sie die Rolle zentraler Clearingstellen als Mittler ersetzen oder verändern können. Da die Technologie und deren Anwendungen noch jung und zum Teil erst im Entstehen sind, gibt es noch wenige Erfahrungswerte. Einige neue Anwendungen sind schon heute machbar und tragfähig. An anderen Anwendungen wird – auch in Berlin – intensiv entwickelt. Um neue Rollen für Mittler zu schaffen, benötigen einige Anwendungsmöglichkeiten allerdings erhebliche Netzwerkeffekte, die in so einem frühen Stadium der Technologie noch nicht abzuschätzen sind.

(3) Was technisch grundsätzlich möglich ist, unterscheidet sich in manchen Branchen von dem, was derzeit aus regulatorischer Sicht eindeutig geregelt ist. Hier besteht branchenspezifischer Klärungsbedarf. Des Weiteren sind Entwickler und Unternehmer mit einem gewissen Grad an Rechtsunsicherheit konfrontiert, da die Realität des Internets sowie öffentlicher Blockchains und die unterschiedliche nationalstaatliche Gesetzgebung stark auseinander klaffen. Neuartige Anwendungen und Organisationsformen wie dApps oder DAOs werfen gesellschaftsrechtliche Fragen auf, die noch zu klären sind. Für Smart Contracts, die Verträge in Form von Programmcode sind, fehlt noch ausreichende Erfahrung in der Rechtspraxis, wie diese rechtssicher gestaltet werden können.

(4) Berlin ist einer der Hotspots weltweit, an dem sich eine Vielzahl von Blockchain Entwicklern und Blockchain Startups konzentrieren. Es werden Maßnahmen aufgezeigt, wie man den Technologiestandort Berlin in dieser Hinsicht weiter stärken könnte. Die Studie empfiehlt möglichen öffentlichen und privaten Anwendern konkrete Pilotprojekte zur Evaluation der Technologie, insbesondere im Bereich des e-Government, des dezentralen Energiehandels und im Bereich transparenter Supply Chains.

Executive Summary

Blockchain is a new technology for the verification of data transactions. It is a type of distributed data storage and processing that enables many features of centrally organized information systems to be decentralized. The Blockchain can be used everywhere where information is to be stored and verified and where usually an intermediate agent is engaged. A Blockchain is a shared, trusted, public record of transactions, that everyone can inspect, but which no single user controls. It is an encrypted, secure, tamper resistant, distributed database. It solves a complex mathematical problem and allows us to build anything from simple Smart Contracts, to whole dApps (Decentralized Applications) or complex DAOs (Decentralized Autonomous Organizations) on top of it. It is considered by many to be a game changer that allows us to decentralize trust, creating the basis for a peer-to-peer economy, powered by auto enforceable smart contracts. Transactions on the Blockchain through these smart contracts are in many cases faster and cheaper and more secure than transactions that classically run through neutral central authorities.

Blockchain can be seen as one of the most important building blocks of the next generation Internet. If the WWW revolutionized information, and the Web2 introduced the programmable Web through Social Media and the Sharing Economy, Blockchain can be seen as the most important building block in the Web3, the decentral web, allowing for real P2P transactions without a middle man.

This report explains Blockchain as a technology, analyses potential use cases, lines out relevant players in Berlin, and defines an action plan to strengthen the local ecosystem. The first part will give an introduction to Blockchain as a technology without going into too many technical details. The second part will showcase selected applications and discuss industry sectors where Blockchain could be relevant: Banking and Finance, Creative Industries, Sharing Economy, Energy Sector, eGovernment, Legal Tech, Health, and IT Consulting. The last part of this report will focus on Berlin as an Innovation Hub, analyzing the current ecosystem and players active in the field.

Most important learnings are:

- (1)** Blockchain technologies can substitute applications based on centralized trust authorities or clearing houses. Security and vulnerability of Blockchain technologies differ substantially from conventional solutions.
- (2)** Blockchain technologies can be used in a broad spectrum of industries. They enable new ways of organizing business transactions by substituting intermediary agents or by changing their roles. As the technology is new and many applications are just being developed there is a lack of experience to overcome. Some applications are technically feasible and stable. Others still are intensely engineered, many of them in Berlin. To take disruptive effects on the role of intermediary agents, some applications will need considerable network effects that can't be estimated in the current early stage of the technology.
- (3)** Developers and Entrepreneurs currently face many legal uncertainties, since the reality of the internet and the different national legal frameworks diverge. New types of organizations like dApps or DAOs pose new challenges for companies laws that remain to be solved. Smart contracts, being contracts in form of programmed code, pose new challenges, because there is a lack of practice on how such contracts can be closed in a legally compliant and binding form.
- (4)** Berlin is an international hotspot for many Blockchain developers and Blockchain startups. This report shows, how Blockchain technology in Berlin can be further strengthened and recommends pilot projects for the further evaluation of the technology, especially in the sectors of eGovernment, decentralized energy trading, and transparent supply chains.

1. Über Blockchain

Blockchain ist eine neue Technologie der Verifizierung von Datentransaktionen. Es handelt sich um eine Form der Verteilung und Sicherung von Daten, auf deren Basis viele Funktionen zentral organisierter Informationssysteme dezentralisiert werden können. Die Blockchain kann überall dort zum Einsatz kommen, wo es normalerweise eines Vermittlers, einer ‚Trusted 3rd Party‘, bedarf, wo Informationen sicher verwaltet und verifiziert werden müssen. Blockchain bietet Nachvollziehbarkeit sowie (statistische) Fälschungssicherheit¹, ohne bei einer unabhängigen, zentralen Instanz anfragen zu müssen.

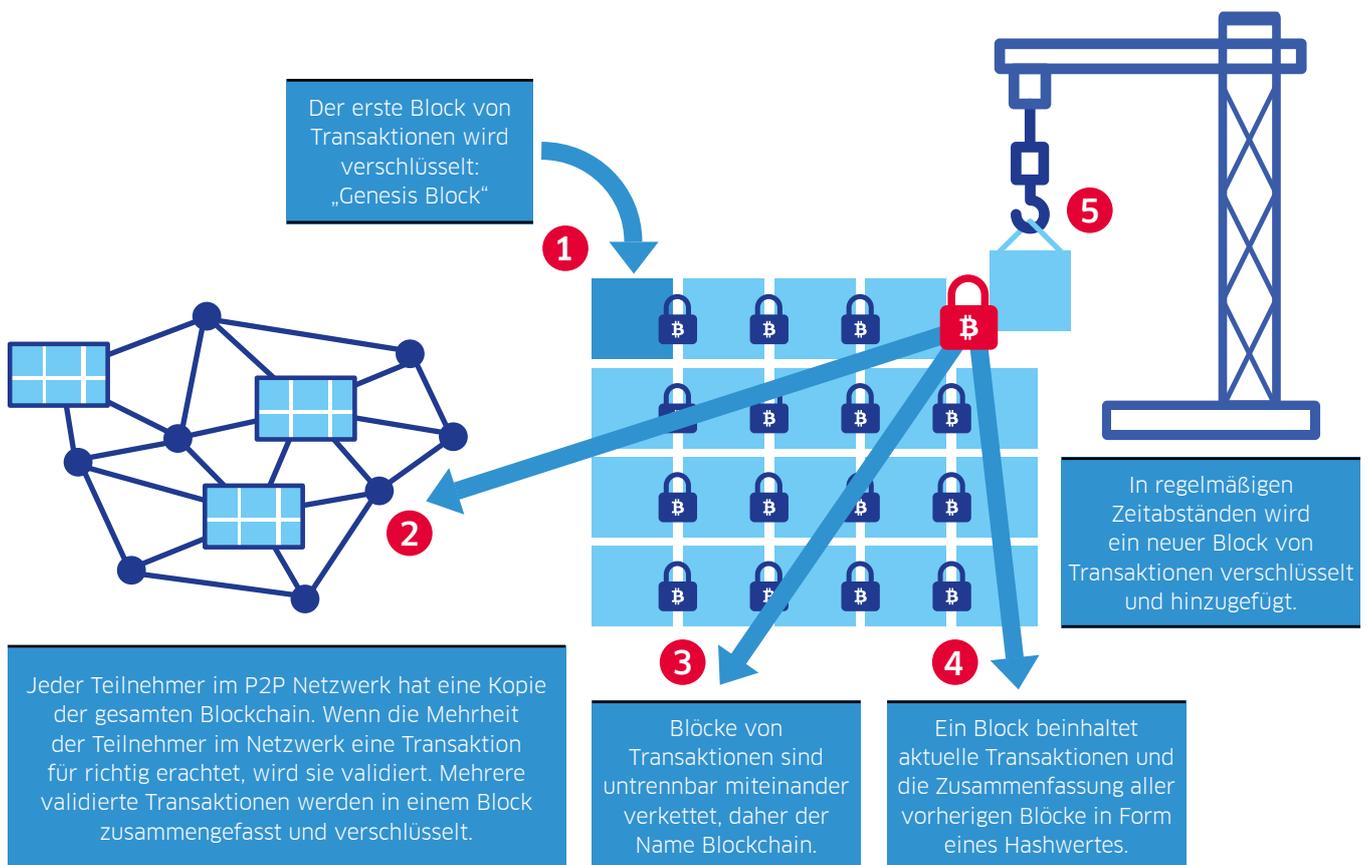
Die Blockchain ist eine auf vielen Computern gleichzeitig gepflegte Datei, in der sämtliche Transaktionen aller Teilnehmer vom gesamten Netzwerk per Mehrheits-Konsens validiert und abgespeichert werden. Einmal abgespeichert kann eine Transaktion im Nachhinein nicht mehr verändert werden. Transaktionen werden in Blöcken verschlüsselt und sind miteinander verkettet, daher der Name Blockchain.

Blockchain Technologien ermöglichen erstmals, dass wir digitale Werte nicht von A nach B kopieren, sondern sie über ein dezentralisiertes Netzwerk so transferieren, dass jeder Teilnehmer des Netzwerks zweifelsfrei und anonymisiert feststellen kann, wer gerade im Besitz des Wertes ist.²

Auf Blockchain basierende **Smart Contracts**, **dezentralisierte Anwendungen (dApps)** und **Dezentral Autonome Organisationen (DAOs)** können herkömmliche „Trusted 3rd Parties“ ersetzen, sowie wirtschaftliche und bürokratische Transaktionen unterschiedlichster Natur um ein vielfaches billiger, schneller und sicherer als herkömmliche zentralisierte Client-Server-basierte Informationssysteme machen. Um die Bedeutung und das Potenzial von Blockchain besser verstehen zu können, ist es hilfreich, einen kurzen Blick in die Geschichte des Computers und des Internets zu werfen.

Abbildung 1

Blockchain: Woher stammt der Name?



Quelle: eigene Darstellung

1 Statistische Fälschungssicherheit: zur Fälschung muss die Mehrheit der an einem P2P-Netz teilnehmenden Knoten kompromittiert werden. Das macht Fälschungen nicht inhärent unmöglich, erhöht den Aufwand aber enorm.

2 Bitcoin Kurz & Gut, Jörg Plutzer, 2014, Seite 65 (Kindle Version)

1.1 Blockchain und die Entwicklung des Web

Wenn man an die Anfänge der Computergeschichte denkt, so gab es zuerst Mainframe Computer. Sie waren groß, mussten von mehreren Menschen bedient werden und nur wenige private und staatliche Institutionen konnten sich Computer überhaupt leisten. Mit dem Einzug des Personal Computers in private Haushalte in den 1980er Jahren änderte sich alles schlagartig. Obwohl es das Arpanet - den Vorläufer des Internets - schon seit den 1960er Jahren gab, waren die meisten Computer weltweit bis Anfang der 1990er Jahre nicht miteinander verbunden.

Erst die Entwicklung des TCP/IP Protokolls Anfang der 1980er Jahre und der darauf folgende Aufstieg des Internets Anfang der 1990er ermöglichten die zunehmende Vernetzung der Rechner weltweit, zunächst von privaten Haushalten, Firmen und anderen Institutionen. In weiterer Folge kam die Vernetzung mit mobilen Endgeräten dazu. Mit dem Internet der Dinge vernetzten sich in einem nächsten Schritt immer mehr autonome Geräte miteinander.

Die ersten sogenannten Killer-Anwendungen Anfang der 1990er Jahre waren Email (SMTP) und das World Wide Web (HTTP). Trotz weiter Verbreitung des Internets und der Vernetzung von Milliarden Endgeräten, wurden und werden die meisten Daten weiterhin zentral gespeichert und im Client-Server Prinzip gesichert, verarbeitet und abgefragt.

Das Internet auf Basis des TCP/IP Protokolls war zwar ein erster Schritt in Richtung Dezentralisierung, indem es den Zugang zu Information und den Datenaustausch vereinfacht und beschleunigt hat. Allerdings werden Daten auch heute noch in den meisten Fällen zentral gespeichert: entweder direkt auf dem Computer oder den jeweiligen Endgeräten oder remote in der sogenannten Cloud. Doch auch die Cloud basiert auf zentraler Datenspeicherung: Die Daten werden via Internet auf Servern gespeichert, auch wenn diese verteilt sein können und es nicht relevant ist, wo sie sich befinden.

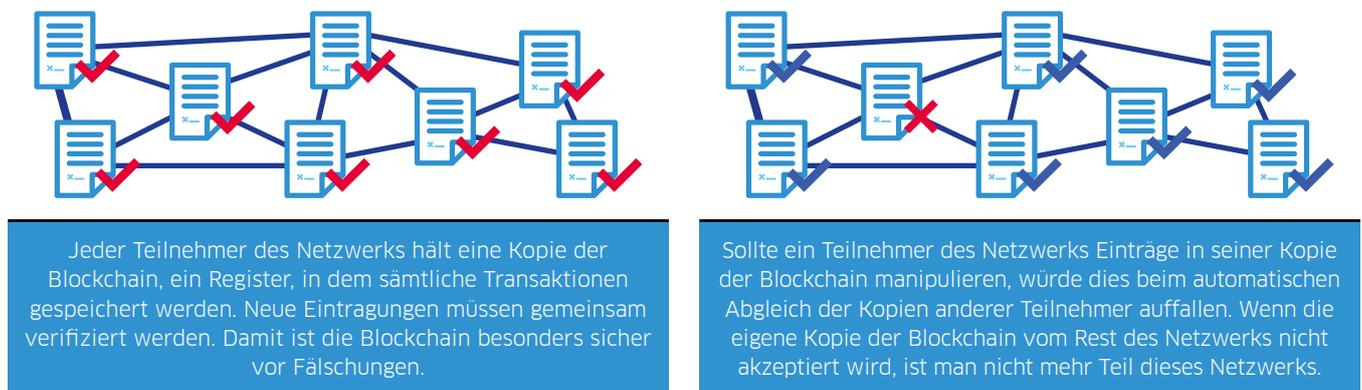
Eine Herausforderung bei zentraler Datenspeicherung besteht darin, dass Datensicherung, Verifizierung und Zertifizierung von Transaktionen geld- und zeitintensiv sind und immer eine potenzielle, zentrale Quelle für Fehler, Manipulation und Zensur darstellen. Diese können intern oder extern verursacht sein, absichtlich oder unabsichtlich, durch Mensch oder Maschine.

P2P³-Netzwerke, die Ende der 1990er durch Anwendungen wie Napster populär wurden, zeigten erstmals einer breiteren Öffentlichkeit, wie man in einer vernetzten Welt neue Datenstrukturen schaffen kann, die in einer Welt der alleinstehenden, nicht vernetzten Computer bislang nicht möglich gewesen waren.

Blockchain baut unter anderem auf der Logik der P2P-Netzwerke auf, löst das Problem der zentralen Datenspeicherung und Transaktionsvalidierung und ist somit möglicherweise der nächste große Schritt in der Entwicklung der Computer und des Internets.

Abbildung 2

Warum ist die Blockchain fälschungssicher?



Quelle: eigene Darstellung

3 P2P (= peer to peer): An einem P2P-Netzwerk teilnehmende Computer sind über die physische Struktur des Internets ohne zentrale Instanzen und gleichberechtigt miteinander verbunden und können Daten direkt untereinander austauschen oder verteilt verarbeiten. Jeder Computer in diesem Netzwerk ist sowohl Server als auch Client. Zentrale Instanzen sind nicht erforderlich.

1.2 World Wide Web

Das WWW hat den Informationsaustausch revolutioniert. Das sogenannte Web2 baut mit neuartigen Anwendungen auf dem WWW auf: Social Media haben neue Kommunikations- und Interaktionsformen geschaffen. Online Marktplätze haben Käufer und Verkäufer weltweit einander näher gebracht, Vertriebswege verkürzt und komplett neue Anwendungsfelder kreiert, unter anderem die sogenannte Sharing Economy. Das Dezentrale Web, von vielen innerhalb der Entwickler Community auch Web3 genannt, hat das Potenzial, den Wertaustausch zu revolutionieren.

Information Data Highway, das statische Web, Web1 oder WWW: Im Grunde genommen basiert das Internet, wie wir es heute kennen, auf einem Protokoll: dem TCP/IP. Alle anderen Protokolle und Dienste, die danach kamen, bauten darauf auf. Datenautobahn war das Schlagwort der 1990er. Heute verwendet niemand mehr dieses Wort, weil es selbstverständlich geworden ist, dass wir immer und allgegenwärtig mit allen anderen verbunden sind und kommunizieren. Anfang der 1990er Jahre konnte zwar so mancher schon ahnen, was für ein bahnbrechendes Potenzial das Internet hat. Die wenigsten aber haben die Entwicklung der letzten 25 Jahre vorhersehen können. Viele Dinge, die wir heute als selbstverständlich ansehen, waren in den 1990er Jahren noch reine Science Fiction.

Das programmierbare Web, Social Media, Sharing Economy oder Web2: Um die Jahrtausendwende kam mit dem Web2 der nächste Entwicklungsschritt. Im Web2 wurde das Internet programmierbar. Die Weiterentwicklung von Informationsaustausch erfolgte durch komplexe Anwendungen, die auf den einfachen Internet Protokollen aufsetzten und eine neue Form der Interaktion ermöglichten. Social Media Anwendungen wie Myspace, Facebook, Youtube, Twitter und alles, was danach kam, haben die Form der Kommunikation von bilateral auf multilateral geändert. Jeder war plötzlich ein Sender von Informationen in einer noch komplexeren Art, als es zuvor mit Email und statischen Webseiten möglich gewesen war. Die Grenze zwischen Konsumenten und Produzenten verfließ. Online Marktplätze haben Vertriebswege verkürzt. Secondhand wurde plötzlich salonfähig. Die Sharing Economy hat neue Geschäftsmodelle geschaffen: Mieter und Wohnungsbesitzer

wurden zu Teilzeithoteliers, jeder Autobesitzer wurde zum potenziellen Taxifahrer, jeder Smartphonebesitzer zum Citizen Journalist. Transparenz und Transaktionskosteneffizienz haben diese Entwicklung begünstigt. Dies war ein erster Schritt in Richtung P2P-Ökonomie, aber immer mit einer zwischengeschalteten Clearingstelle, einer vertrauenswürdigen Plattform als Mittelsmann. So sehr diese neuen Plattformen Menschen und Institutionen weltweit einander näher brachten, wurde dadurch aber auch ein neues Problem geschaffen: die zunehmende Marktdominanz einiger weniger Plattformbetreiber wie Ebay, Amazon, Zalando, Airbnb, Uber, Facebook, Twitter, u.a.. Daten, die auf den zentralen Rechnern dieser Firmen gespeichert werden, sind zu einer wertvollen Handelsware für die Werbebranche geworden, eine indirekte Einnahmequelle für die Plattformbetreiber. Nutzer geben einerseits die Rechte an ihren privaten Daten auf (vor allem relevant im Zusammenhang mit Social Media) und sind darüber hinaus von der Marktmacht der Plattformbetreiber abhängig (vor allem relevant im Zusammenhang mit Marktplätzen).

Das Dezentrale Web, das autonome Web, Web3: Blockchain kann in dieser Entwicklungsreihe als ein Baustein des Web3 gesehen werden, der den Wertaustausch revolutionieren kann. Blockchain ist ein Transaktionsprotokoll (value exchange protocol), das echte P2P-Transaktionen ermöglicht, und zwar ohne zentrale Clearingstelle oder Trusted 3rd Party. Auf dieses Transaktionsprotokoll können Smart Contracts, dezentrale Anwendungen (dApps) und Dezentrale Autonome Organisationen (DAOs) aufbauen. Im Dezentralen Web vermischen sich die Funktionen des Computers mit Funktionen des Internets. Ein verteiltes Netzwerk von Rechnern übernimmt klassische Funktionen des physischen Rechners. Dafür bedarf es einer Vielzahl neuer Protokolle. Blockchain ist nur eine von vielen Technologien, die ein Dezentrales Web ermöglichen, scheint aber derzeit eine starke Triebfeder dieses Wandels zu sein. Die Blockchain übernimmt im Gesamtsystem des Dezentralen Webs unter anderem die Aufgabe der Prozessorleistung eines dezentralen Computers⁴. Aber ohne komplementäre dezentrale Protokolle wird ein wirklich dezentrales Netz nicht funktionieren. Ausgewählte Bestandteile eines Gesamtsystems Web3 zeigt folgende Abbildung.

⁴ "Prozessor" bzw. "Prozessorleistung" meint hier ganz im wörtlichen Sinne die Leistung des Prozessierens von Datenveränderungen und ist nicht zu verwechseln mit dem Hardwarebauteil CPU (central processing unit), einem Prozessor als Bauteil. Ebenso meint "Computer" hier die Gesamtheit aller verteilten Rechensysteme, nicht etwa einzelne Elektrogeräte auf oder unter Tischen.

Abbildung 3

Dezentrales Web schematisiert als dezentraler Computer



Quelle: eigene Darstellung

Viele dieser Protokolle, Technologien und Anwendungen rund um Blockchains befinden sich noch in den Kinderschuhen. Welche Standards sich letztendlich durchsetzen werden und wann sie eine kritische Masse erlangen, weiß man derzeit noch nicht.

Trotz Blockchain und anderen dezentralen Protokollen wird es auch in Zukunft eine Existenzberechtigung für Clearingstellen und zentralisierte Client-Server-basierte Systeme geben. Nur wird wahrscheinlich die Bedeutung zentralisierter Instanzen tendenziell abnehmen. Ihre Rolle wird sich verändern, während die Bedeutung dezentraler Lösungen zunimmt.

1.3 Technologie hinter Blockchain

In der Blockchain werden Transaktionen unveränderbar und für alle nachvollziehbar abgespeichert.⁵ Die Blockchain kann als dezentrales, allumfassendes und transparentes Kontobuch gesehen werden, das alle Transaktionen zwischen Nutzern registriert und die gespeicherten Transaktionsdaten blockweise verschlüsselt und aneinanderreihet. Alle Teilnehmer des Netzwerks haben gleichermaßen Zugriff auf dieselben Daten und zwar in Echtzeit.

Das Validieren von Transaktionen erfolgt dezentral durch das gesamte Netzwerk. Wenn die Mehrheit des Netzwerks eine Transaktion validiert, wird die Transaktion dauerhaft in die Blockchain geschrieben. Ansonsten wird die Transaktion abgelehnt und geht nicht durch.

Das Blockchain Protokoll gibt hierbei den Netzwerkteilnehmern die 'Spielregeln' für das Validieren der Transaktionen vor. Bei öffentlichen Blockchains kann jeder das Protokoll auf seinen Rechner laden und Teil des Netzwerks werden. Bei privaten Blockchains und Konsortium Blockchains ist eine Teilnahme nur auf "Einladung" oder "Erlaubnis" möglich. Grundsätzlich gilt: je mehr Netzwerkteilnehmer es gibt und je diversifizierter diese sind, desto vertrauenswürdiger ist das System.

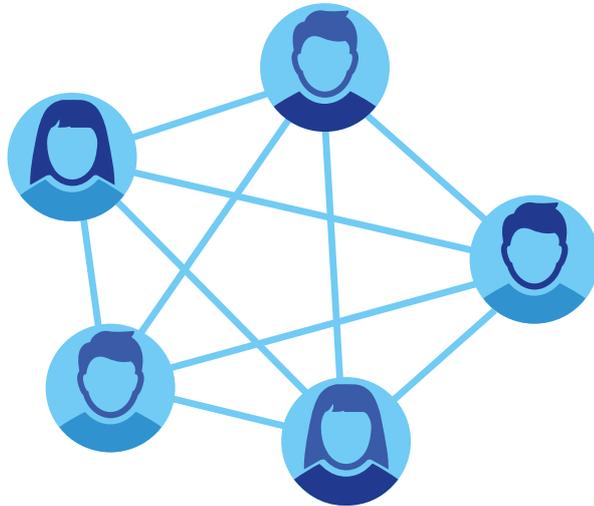
Eine zentrale Fehlerquelle sowie Manipulation und Zensur durch eine zentrale Institution sind somit abgeschafft. Man vertraut nicht einer Person oder Institution, sondern dem Protokoll und den Netzwerkteilnehmern, die Transaktionen dem Blockchain Protokoll entsprechend verifizieren.

Abbildung 4

Vertrauen in Serverbetreiber versus Vertrauen in die Programmierung des Protokolls und die Verifizierung durch peers.



Server = Datenmonarchie



P2P Netzwerke = Datendemokratie

Quelle: eigene Darstellung

Abbildung 5

Die wissenschaftlichen Grundlagen von Blockchain-Technologien



Quelle: eigene Darstellung

P2P-Netzwerke: Transaktionen sind transparent. Alle jemals durchgeführten Transaktionen werden in einem Register gespeichert. "Alle Teilnehmer einer Blockchain sind über ein Peer-to-Peer Netzwerk verteilt und Transaktionen sind für jeden Teilnehmer einsehbar. Damit können alle Transaktionen bis zu ihrem Ursprung zurückverfolgt werden."⁵

Kryptografie sorgt für Transparenz und Privatsphäre gleichermaßen. Über kryptographische Funktionen sind einzelne Transaktionen verschlüsselt. Das verschafft (relative) Anonymität⁶. Blöcke von Transaktionen sind untrennbar miteinander verkettet. Eine Aneinanderreihung von verketteten Transaktionsblöcken wird daher Blockchain genannt. Einzelne Blockchains können mehr Informationen enthalten als die Transaktionsblöcke.⁷ Die Blöcke erhalten neben einer oder mehreren Transaktionen auch eine Zusammenfassung aller vorherigen Blöcke in Form eines Hash Werts⁸. Dieser Hash Wert dient als Fälschungssicherung, mit der die Echtheit einer Transaktionskette überprüft werden kann. Bei Manipulationsversuchen würde der Hash Wert nicht mehr stimmen. Jeder Teilnehmer im Netzwerk darf neue Einträge zur Blockchain hinzufügen. Diese Einträge sind schreibgeschützt und können im Nachhinein nicht mehr verändert oder entfernt werden. Was einmal in die Blockchain geschrieben wird, kann nicht mehr

verändert oder gelöscht werden, es sei denn, die Mehrheit der Teilnehmer stimmt dem zu. Um Transaktionen durchführen zu können, erhält jeder Teilnehmer der Blockchain einen privaten und einen öffentlichen Schlüssel. Der öffentliche Schlüssel stellt eine eindeutige Adresse (eine Art Kontonummer) dar, die als Empfangsadresse für eingehende Transaktionen verwendet wird. Der private Schlüssel muss geheim gehalten werden. Er funktioniert wie ein Passwort. Mit dem privaten Schlüssel werden ausgehende Transaktionen bestätigt. Für eine Transaktion muss der Absender lediglich den öffentlichen Schlüssel des Empfängers angeben, sowie über seine notwendigen privaten Schlüssel für die zu transferierenden Einheiten oder zu bestätigenden Informationen verfügen. Da für eine Transaktion keine weiteren Informationen benötigt werden, müssen die Teilnehmer im Netzwerk nicht mit ihren Klarnamen oder einer geprüften Identität auftreten. Die Blockchain erlaubt daher nicht nur Transparenz, sondern auch eine "relative Anonymität".⁶ Das für die jeweiligen Anwendungen erwünschte Level von Transparenz und Anonymität kann durch entsprechende Programmierung der im Einzelfall verwendeten Blockchain und der zugehörigen Protokolle festgelegt werden und ist auch bei aktuell in Anwendung befindlichen unterschiedlichen Blockchains recht verschieden.⁹

5 ÖFIT-Trendschau: Öffentliche Informationstechnologie in der Digitalen Gesellschaft, Trendthema 36: Blockchain, Mai 2016 (Jens Fromm, Mike Weber, Fraunhofer Fokus)

6 Relative Anonymität: Auf der Bitcoin Blockchain beispielsweise, ist die Zuordnung des Schlüssels zu einer bestimmten Person, für einen normalen Nutzer nicht so einfach möglich, aber mit viel Aufwand durchaus nachvollziehbar (mittels Datadaming). Fälle, in denen dies Ermittlungsbehörden gelungen ist, sind bekannt. Die Blockchain Technologie ist hier aber einem rasanten Wandel unterworfen. Neuere Blockchains, wie Monero und Zcash, haben Protokolle entwickelt, bei denen die Identität einer Adresse gänzlich anonymisiert ist.

7 Zum Beispiel die Bitcoin-Blockchain, die auch die Bitcoins selbst enthält.

8 Ein Hash-Wert ist eine Prüfsumme, die aus dem zu prüfenden Inhalt selbst errechnet wird. Würde der Inhalt verändert, stimmte der Hash-Wert nicht mehr. In der analogen Welt seit Jahrzehnten als "Prüfziffer" z.B. bei Kontonummern und Ausweisdokumenten in Gebrauch.

9 ÖFIT-Trendschau: Öffentliche Informationstechnologie in der Digitalen Gesellschaft, Trendthema 36: Blockchain, Mai 2016 (Jens Fromm, Mike Weber, Fraunhofer Fokus)

Spieltheoretische Incentivierung: Ökonomische Anreizsysteme sorgen dafür, dass die Teilnehmer im Netzwerk im eigenen Interesse für ein funktionierendes Gesamtsystem sorgen: Proof of Work (PoW), Proof of Stake (PoS), Proof of Burn (PoB), u.v.m. Einzelne Teilnehmer im System sind hierbei ökonomisch incentiviert, Transaktionen dem Protokoll entsprechend zu verifizieren. Proof of Work ist bisher am weitesten verbreitet und funktioniert folgendermaßen: Wenn ein Block von Transaktionen korrekt, d.h. dem Protokoll gemäß, verifiziert wird, bekommt der Teilnehmer im Netzwerk einen Block Reward. Incentivierung führt im Zusammenspiel mit dem P2P-Charakter der Blockchain dazu, dass der Aufwand für Manipulationen des Gesamtsystems dann enorm groß wird, wenn die Zahl der beteiligten Nutzer groß ist. Um bestehende Transaktionen, die in der Blockchain gemacht wurden, zu zensurieren oder zu fälschen,

müsste man über die Mehrheit der Netzwerkteilnehmer verfügen und diese dazu bringen können, Transaktionen nicht dem Protokoll entsprechend zu verifizieren. Der ökonomische Aufwand steht in den allermeisten Fällen mit dem Nutzen nicht im Verhältnis. Fälschung oder Zensur wird dadurch ökonomisch unrentabel. Proof of Work macht eine Blockchain sicher, ist aber auch sehr langsam, d.h. zu wenige Transaktionen pro Sekunde können auf einer PoW-basierten Blockchain abgewickelt werden. Auch wenn sie noch in der Entwicklung sind, zeichnen sich viele unterschiedliche Ansätze ab, wie man diese Skalierungsprobleme bewältigen könnte. Hier besteht grundsätzlich noch viel Forschungs- und Entwicklungsbedarf. Im Laufe der nächsten Jahre könnte sich daher die Grundarchitektur von Blockchains unter anderem auch hinsichtlich der Anreizmechanismen ändern.

1.4 Wofür kann man die Blockchain verwenden?

Smart Contracts¹⁰ sind automatisch ausführbare Programme, die auf der Blockchain aufbauen und vordefinierte Transaktionsregeln im Programmcode abbilden. Eine Transaktion, die über einen Smart Contract läuft, wird automatisch ausgeführt, wenn alle beteiligten Parteien die zuvor definierten Konditionen erfüllen. Dadurch erübrigt sich die Notwendigkeit einer zentralen, zwischengelagerten Instanz, insbesondere wenn die beteiligten Parteien sich nicht kennen und somit auch nicht vertrauen, und senkt zudem die Transaktionskosten.

dApps (Decentralized Applications) sind dezentrale Anwendungen, vom Backend bis zum User Interface, die auf einer Blockchain laufen und einen oder mehrere Smart Contracts verwenden. Die Begriffe dApps und Smart Contracts werden in der noch jungen Blockchain Community unterschiedlich ausgelegt. Definitionen sind einem raschen Wandel unterworfen.

DAOs (Decentralized Autonomous Organizations) sind eine neue Form der Organisation, deren Statuten, Geschäftsordnung, Gesellschaftsvertrag oder Satzung durch einen Smart Contract abgebildet und automatisch ausgeführt werden. Die Spielregeln der Organisation werden im Vorfeld definiert und in die Smart Contracts programmiert. DAOs brauchen kein zentral organisiertes Management des Tagesgeschäfts mehr. Die Rollen von Spezialisten werden durch gewählte Teilnehmer der DAO oder externe "Agenten" übernommen. DAOs sind die höchste und komplexeste Form eines Smart Contracts. Wir befinden uns allerdings in einer sehr frühen Phase der Entwicklung von DAOs. Hier besteht noch viel Forschungs- und Entwicklungsbedarf und es bedarf technologischer Netzwerkeffekte, bevor diese Anwendungen in einer breiten Masse relevant werden können.

¹⁰ Smart Contracts sind nicht 1:1 mit klassischen Verträgen in Textform gleichzusetzen, könnten diese aber solche in Zukunft ersetzen, wenn dem entsprechende Rahmenbedingungen erfüllt sind (siehe Kapitel weiter hinten).

1.5 Welche Blockchains gibt es?

Bitcoin: Obwohl das Konzept von Blockchain und P2P-Netzwerken im akademischen Umfeld schon seit den 1980er Jahren existiert, gab es nie einen Anwendungsfall, der eine bedeutende kritische Masse erreichte. Bitcoin war sozusagen der erste richtige Anwendungsfall einer Blockchain, der in den letzten Jahren zunehmend an Bedeutung gewonnen hat. Auslöser war die Wirtschaftskrise 2008. Der Kollaps der Bank Lehman Brothers stellte den Höhepunkt dieser Krise dar. Was damals für viele erstmals deutlich wurde: Banken sind ein „single point of failure“ und wenn diese zentrale Instanz versagt oder kollabiert, sind die Kollateralschäden groß. Wenige Wochen später publizierte eine anonyme Person oder Gruppe namens Satoshi Nakamoto ein White Paper, in dem Bitcoin als Kryptowährung erstmals definiert wurde. Die Idee hinter Bitcoin war es, funktionsfähiges Geld ohne Banken und Zentralbanken zu kreieren. Freiwillige Programmierer setzten daraufhin dieses White Paper in Code um und wenige Monate später gab es Bitcoin. Das dahinter liegende Protokoll nannte man Blockchain. Aktuelle Zahlen zu Bitcoin: 10 Milliarden USD Marktkapitalisierung, ca. 5 Millionen User.

Altcoins: Das Bitcoin Protokoll sowie das Protokoll anderer öffentlicher Blockchains, die danach kamen, ist open source und kann von jedem kopiert und modifiziert werden. Somit kann jeder auf der Grundlage dieses Codes seine eigene Kryptowährung mit angepassten Variablen kreieren. Im Laufe der Jahre wurde das Bitcoin Protokoll hundertfach modifiziert.¹¹ Man kam schnell auf die Idee, Bitcoin als Transaktions-Token für jegliche Art von wirtschaftlichen und juristischen Verträgen zu verwenden. Eine der spannendsten Entwicklungen hierbei waren Colored Coins und Master Coins. Vitalik Buterin, der einige Zeit an solchen Entwicklungen mitgewirkt hatte, stellte rasch fest, dass diese Anpassungen der Bitcoin Blockchain zwar möglich, aber nicht effizient und flexibel genug waren. Er entwickelte daher das White Paper für Ethereum. Andere Altcoins sind beispielsweise: Dash, Dogecoin, Litecoin, Lisk, Namecoin, Peercoin, Monero, Tendermint, ZCash, u.v.m.¹²

Ethereum ist in dieser Entwicklungsreihe derzeit eine der vielversprechendsten öffentlichen Blockchains. Ethereum ist eine von Bitcoin unabhängige Blockchain. Das Protokoll ist einer komplett anderen Logik unterworfen. Im Gegensatz zu Bitcoin, das für eine einzige Funktion ausgelegt ist (Geld von A nach B schicken ohne zwischengeschaltete Bank), ist die Ethereum Blockchain als ein dezentrales Rechnernetzwerk konzipiert, auf dem man jegliche Art von Smart Contracts und dApps programmieren kann. Im Gegensatz zu Bitcoin ermöglicht die Ethereum Blockchain somit jegliche Art von P2P Wertaustausch, nicht nur Geldtransaktionen. 2013 veröffentlichte Vitalik Buterin das White Paper zu Ethereum, kurz darauf spezifizierte Gavin Wood das Yellow Paper für Ethereum. 2014 folgte eine Crowdfunding Kampagne, in der innerhalb von 6 Wochen 18 Millionen USD in Bitcoin durch Crowdfunding/Crowdinvesting aufgestellt wurden. Im Juli 2015 wurde die Ethereum Plattform gelauncht. Die Ethereum Foundation hat ihren Sitz in der Schweiz. Ein Teil des Entwicklerteams sitzt in Berlin. Ziel der Ethereum Foundation ist es, die Ethereum Blockchain und darauf aufbauende dezentrale Technologien zu entwickeln und kontinuierlich weiterzuentwickeln und der Öffentlichkeit zur Verfügung zu stellen.¹³ Zum technologischen Ökosystem von Ethereum gehören neben der Ethereum-Blockchain eine Vielzahl verfügbarer Clients, mit denen man am System teilnehmen kann, außerdem sind mehrere Programmiersprachen verfügbar, mit denen man Smart Contracts erstellen kann. Viele spannende Projekte und Startups setzen gerade auf die Ethereum - Blockchain, unter anderem slock.it, RWE, Thomson Reuters, Santander Bank, Microsoft, Bitnation, um hier nur einige zu nennen.¹⁴ Im Laufe des nächsten Jahres werden wir die ersten greifbaren Projekte sehen. Es wird voraussichtlich noch einige weitere Jahre dauern, bis das Potenzial der Anwendungen auch in einer breiteren Öffentlichkeit greifbar wird.

11 <http://altcoins.com/>

12 <http://coinmarketcap.com/>

13 Siehe Handelsregisterauszug: <http://www.hrazg.ch/webservices/net/HRG/HRG.aspx/getHRGPDF?chnr=CH-170.7.000.758-1&amt=170&toBeModified=0&validOnly=0&lang=1&sort=>

14 Einige dieser Projekte wurden erstmals auf der Entwicklerkonferenz von Ethereum im September 2016 in Shanghai vorgestellt: https://ethereum-foundation.org/devcon/?page_id=14.

Weiterführende Quellen:

<http://www.coindesk.com/microsoft-ethereum-3-million-developers/>

<http://www.coindesk.com/german-utility-company-turns-to-blockchain-amid-shifting-energy-landscape/>

<http://www.ibtimes.co.uk/bitnation-launches-decentralised-borderless-virtual-nation-constitution-ethereum-1544431>

<https://cointelegraph.com/news/santander-confirms-fiat-backed-token-project-on-ethereum-blockchain>

<http://www.coindesk.com/thomson-reuters-blockoneid-ethereum-blockchain/>

Konsortium Blockchains: Im Gegensatz zur ursprünglichen Idee von einer Blockchain (Protokoll ist open source und jeder kann Teilnehmer des Netzwerks werden), haben einige Branchen angefangen, an Konsortium Blockchains zu arbeiten. Bei Konsortium Blockchains sind die Akteure der Blockchain ausgewählt, nur diese können/dürfen Transaktionen validieren. Wenn daher der klassische Finanzsektor beispielsweise von der Blockchain spricht, so sind meist keine öffentlichen Blockchains wie Bitcoin oder Ethereum sondern eher Konsortium Blockchains gemeint oder private Blockchains (siehe unten), um beispiels-

weise Interbank-Transaktionen effizienter zu gestalten. So eine Lösung entspricht einem Information/Daten Oligopol und ist somit eine Teildezentralisierung von Transaktionsvalidierung.

Private/Enterprise Blockchains: Das sind in-house Lösungen, die darauf abzielen, das Datenmanagement innerhalb eines Unternehmens effizienter zu gestalten. Sie bieten höhere Transaktionssicherheit, Nachvollziehbarkeit und somit weniger Fehler und Redundanzen. Alle Netzwerkteilnehmer befinden sich innerhalb eines Unternehmens. Das Protokoll ist nicht öffentlich.

Abbildung 6

Welche Blockchains gibt es?

Öffentliche Blockchains	Private Blockchains	Konsortium Blockchains
<ul style="list-style-type: none"> · Unendlich viele Netzwerkteilnehmer · Jeder kann Transaktionen validieren · Protokoll öffentlich 	<ul style="list-style-type: none"> · Ausgewählte und begrenzte Anzahl von Netzwerkteilnehmern · Nur ausgewählte Mitglieder können Transaktionen validieren · Protokoll nicht öffentlich 	<ul style="list-style-type: none"> · Netzwerkteilnehmer nur innerhalb eines einzelnen Unternehmens · Nur ausgewählte Mitglieder können Transaktionen validieren · Protokoll kann öffentlich sein (open source) oder nicht öffentlich

Quelle: eigene Darstellung

1.6 Status Quo und langfristiges Potenzial

Blockchain als Technologie gibt es in der jetzigen Form seit 2009. Die Technologie, die ursprünglich für Bitcoin entwickelt wurde, um Geldtransaktionen ohne Banken zu ermöglichen, bietet nun auch das Potenzial für eine Vielfalt von neuen Anwendungen. Die Entwicklung von Blockchain steckt zwar noch in den Kinderschuhen, doch sie vollzieht sich rasant. Immer mehr Unternehmen und Forschungseinrichtungen beschäftigen sich mit dem Thema. Immer mehr Investitionskapital drängt in den Markt.

Genaue Entwicklungen lassen sich derzeit nicht vorhersehen. Anfang der 1990er Jahre war auch noch nicht vorhersehbar, dass wir heute Smartphones haben, auf denen wir Dienste wie Wikipedia, Facebook, Youtube, Twitter u.v.m. verwenden. Damals konnten wir nur Email und das WWW als erste Anwendungen

des Internet. Obwohl vielen schon klar war, dass diese neue Technologie unser Kommunikationsverhalten revolutionieren würde, konnten die meisten das Ausmaß des technologischen, wirtschaftlichen und gesellschaftlichen Wandels, den wir in den letzten 25 Jahren gesehen haben, damals dennoch nicht vorhersehen.

Bei Blockchain verhält es sich ähnlich. Wir stehen erst am Anfang. Mit jeder neuen Anwendung, die auf der Blockchain realisiert wird, mit jeder neuen Firma, die anfängt, Blockchain-basierte Dienste anzubieten, mit jeder neuen Technologie, die auf der Blockchain aufbaut, wird das Potenzial klarer und greifbarer. Wir wissen noch nicht, wann die nächste Killer-Anwendung auf der Blockchain kommen wird. Dass sie aber früher oder später kommen wird, scheint aktuell sehr wahrscheinlich.

2. Branchen und Anwendungsgebiete

Smart Contracts auf der Blockchain ermöglichen zum ersten Mal echte P2P-Transaktionen ohne Mittelsmann und haben das Potenzial, viele bisherige Geschäfts- und Verwaltungsprozesse von Grund auf zu transformieren. Betroffen von dieser Transformation sind Banken, Versicherungen und all jene Behörden, die Informationen archivieren, verifizieren, authentifizieren, lizenzieren, patentieren und zur Verfügung stellen. Betroffen sind aber auch klassische Vertriebsketten. Die Blockchain hat das Potenzial, traditionelle wirtschaftliche Produktions- und Vertriebsketten auf den Kopf zu stellen sowie Mittelsmänner und Zwischenhändler abzuschaffen. Sie kann aber auch sehr viel mehr Transparenz schaffen. Insbesondere haben Blockchain-basierte Verfahren das Potenzial, Anwendungen aus dem Bereich der Sharing Economy

oder sogenannter Prosumer-Modelle, die im Kern peer-to-peer Geschäfte sind und heute durch Plattform Betreiber vermittelt und abgewickelt werden, ein peer-to-peer Abwicklungssystem zur Verfügung zu stellen. Somit würde die Notwendigkeit der Rolle des Plattform-Betreibers in der herkömmlichen Art und Weise abgeschafft oder zumindest stark verändert werden.

Des Weiteren könnte sich Blockchain auch zur Basistechnologie für klassische Industrie 4.0 Lösungen entwickeln. In einer IoT Welt, in der Maschine-zu-Maschine Kommunikation und Transaktion essentiell sind, bieten Smart Contracts auf Blockchain Basis durch ihre automatisierte Vertragsabwicklung eine effiziente Lösung.

Abbildung 7

Anwendungspotenziale von Blockchains nach Branchen

Anwendungspotenziale von Blockchains
Energiewirtschaft
Datensicherheit und Transparenz
Banken, Versicherungen und FinTech
Kreativwirtschaft
IoT und Industrie 4.0
Verwaltung und eGovernment
Mobility
Legal Tech

Quelle: eigene Darstellung

2.1 Banken, Versicherungen und FinTech

Der klassische Finanzsektor hängt in seiner Transaktionseffizienz zum Teil Jahrzehnte hinter den technischen Möglichkeiten nach, und das schon lange bevor es die Bitcoin gab. Dies hat in den vergangenen Jahren dazu geführt, dass FinTech Startups weltweit den klassischen Banken merklich Marktanteile durch effizientere, schnellere und günstigere Transaktionen abgraben konnten.

Während heutzutage beispielsweise High Frequency Trading zur Selbstverständlichkeit geworden ist, wobei in Millisekunden Wertpapiere in Milliardenhöhe gehandelt werden, dauert es dennoch mehrere Tage, bis der Handel dieser Wertpapiere formal abgewickelt ist. Banküberweisungen, auch innerhalb eines Landes, dauern mehrere Tage, während man mit Bitcoin in wenigen Sekunden Geldbeträge von Europa nach Afrika schicken kann. Zu einem Bruchteil der Transaktionskosten normaler Banküberweisungen wohlgemerkt. Dieser Kosten- und Geschwindigkeitsvorteil entsteht dadurch, dass Transaktionen peer-to-peer ausgeführt und abgewickelt werden und nicht mehrere Server und Clearingstellen mit semiautomatischen Compliance-Prüfungen durchlaufen müssen, wie es im Finanzbereich sonst üblich ist. Ein zusätzlicher Vorteil ist, dass bei internationalen Transaktionen Währungsumrechnungen beim Zahlungsvorgang entfallen. Somit werden erstmals Mikrotransaktionen rentabel. Dies wird über den FinTech Sektor hinaus Wellen schlagen und Auswirkungen auf neue Produkte und Dienstleistungen haben, die bis dato einfach nicht rentabel waren.

Diese Mängel haben nun auch viele Banken erkannt. Sie versuchen zu identifizieren, inwieweit sie private sowie Konsortium

Blockchainlösungen einsetzen können, um ihre Geschäftsprozesse zu optimieren. Die Bank Santander beispielsweise hat errechnet, dass sie bis zum Jahr 2030 20 Milliarden USD¹⁵ durch den Einsatz von Blockchain Technologien einsparen könnte. Für den Kunden ist das kein wesentlicher "Disrupt". Der Mehrwert für die Bank ist Wettbewerbsfähigkeit mit den jungen FinTechs durch Prozessoptimierung und günstigere Transaktionskosten, die dann zum Teil auch an die Kunden weitergegeben werden können.

R3 beispielsweise ist ein Konsortium von 42 der international größten Banken, die den Nutzen der Blockchain für Banken ergründen und gemeinsame Standards entwickeln. Deutsche Bank, Commerzbank und UBS sind unter anderem an diesem Konsortium beteiligt. Bei diesem Konsortium Blockchains handelt es sich allerdings nicht um eine komplette Dezentralisierung von Transaktionsvalidierung, sondern um eine Dezentralisierung innerhalb eines strikt definierten Konsortiums.

Neuere Fintech Startups gehen aber zum Teil ganz andere Wege und es bleibt abzuwarten, was hier in den nächsten Jahren noch auf uns zukommen wird. Die auch in Berlin tätige Firma Bitwala bietet Finanzdienstleistungen rund um Bitcoin, die eine bessere Bedienungsfreundlichkeit von Bitcoin und eine bessere Schnittstelle mit klassischen Finanzdienstleistungen beinhalten. Unter anderem ermöglichen sie SEPA-Überweisungen mit Bitcoin. Die ebenfalls in Berlin ansässige Firma SatoshiPay bietet Nanopayments auf der Bitcoin Blockchain an, die insbesondere für das Verlagswesen und im IoT Bereich relevant werden können.

¹⁵ <http://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/>

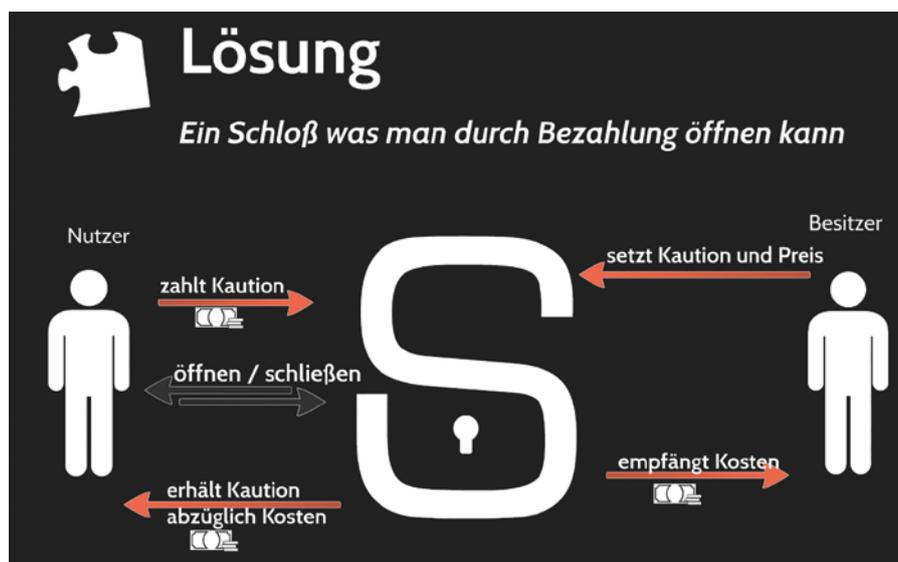
2.2 Sharing Economy, Internet of Things und Industrie 4.0

Smart Access Control Lösungen, wie sie die deutsche Firma slock.it bietet, bauen auf der Ethereum Blockchain auf. Smart Locks sind eine praktische Lösung für die Sharing Economy. Mit slock.it kann man alles vermietbar machen, was den modernen Menschen umgibt: Wohnungen, Autos, Waschmaschinen, Fahrräder, Rasenmäher. All diese Geräte haben in Zukunft ein digitales Schloss, das Transaktionen über die Blockchain verifiziert, und jeder meiner autorisierten Nachbarn kann nun meine Geräte verwenden. Die Vermietung wird über slock.it mittels Smart Contracts auf der Ethereum Blockchain effizient, kostengünstig und allgemein nachvollziehbar abgewickelt. Das ist die Vision von slock.it, die eine Sharing Economy mit angemessen geringem Verwaltungsaufwand ermöglichen könnte.

Einer der spannendsten Anwendungsfälle für Blockchain ist das Internet der Dinge und Industrie 4.0. Mit dem Internet der Dinge sollen all jene Endgeräte des täglichen Gebrauchs miteinander vernetzt werden und interagieren, die bisher nicht miteinander vernetzt waren. Smart Contracts auf der Blockchain sind hierbei eine ideale Ergänzung dieser Entwicklung. Da das Internet der Dinge auch in der Produktion Einzug halten soll -unter anderem sollen in der Industrie 4.0 Werkstücke ihre eigene Bearbeitung durch direkte Kommunikation mit den Bearbeitungsmaschinen steuern- darf damit gerechnet werden, dass Industrie 4.0 ebenfalls zu einem der spannendsten Anwendungsfälle für Blockchain werden kann. Smart Contracts auf der Blockchain sind hierbei eine ideale Ergänzung dieser Entwicklung, da sie für die Übergabe korrekter Produktionsanweisungen an Maschinen sehr geeignet erscheinen ebenso wie für die Abrechnung von Produktionsschritten und Kontrolle auf vertragsgemäße Erfüllung.

Abbildung 8

Peer-to-Peer-Economy, Verleih und Bezahlung mit slock.it



Quelle: www.slock.it

2.3 Sharing Economy und Kreativwirtschaft

Heutzutage kann jeder mit seinem Smartphone oder auf dem Computer schneller und billiger denn je Filme, Musik und Texte produzieren und durch die sozialen Netzwerke jedem anderen Verbraucher weltweit zur Verfügung stellen. Diese Entwicklung hat in den vergangenen Jahren ganze Industrien in den Umbruch gestürzt und neue Marktteilnehmer generiert. Eine neue Mischform von Nutzer und Produzent ist entstanden: der Prosumer. Durch Digitalisierung von Medieninhalten sowie das Web2 wurden Verbraucher plötzlich auch zu Produzenten von Musik, Nachrichten und Filmen. Die klassischen Player in der Kreativwirtschaft, im Verlagswesen, in Film- und Fernsehen oder Musikindustrie haben Marktanteile an neue Marktteilnehmer verloren, an Katzenvideos, Ted Talks, Instagram, musica.ly oder Videoblogger, die plötzlich größere Zuschauerzahlen hatten als etablierte Prime Time Sendungen im TV.

Doch obwohl die Produktion von kreativen Inhalten demokratisiert wurde, ist der Vertrieb dieser neuen Plattformen weiterhin zentralisiert und ein großer Teil der Werbeeinnahmen geht an Firmen, die meist im Silicon Valley sitzen, und nicht an die Produzenten der Inhalte. Blogger sind von den Werbeeinnahmen der Plattformen wie Facebook und Youtube abhängig und können schwer unabhängig von diesen Plattformen Geld verdienen. Blockchain eröffnet hier neue Geschäftsfelder und P2P-Möglichkeiten zu wesentlich niedrigeren Transaktionskosten.

Allerdings sind die Geschäftsmodelle hier unklar, da Daten nicht auf Servern gespeichert werden, Transaktionen nicht zentral validiert werden und der Quellcode open source ist. Wie kann man damit Geld verdienen? Diese Frage ist noch weitgehend unbeantwortet. Genauso wie Anfang der 1990er Jahre nicht absehbar war, wie man mit Online-Content Geld verdient. dApp basierte potenzielle Konkurrenten für bestehende Plattformen werden aber wahrscheinlich erst dann eine kritische Masse von Nutzern erreichen können, wenn sie auch gute User Interfaces haben und genug Geld in Marketing investieren. Die Netzwerkeffekte bestehender Plattformen sind nicht zu unterschätzen. Ob und wie diese neuen, dezentralen Anwendungen auf der

Blockchain auch dazu beitragen können, Prosumern einen ähnlich hohen Reach zum Konsumenten zu ermöglichen, wie bestehende etablierte Plattformen ihn haben, oder ob Blockchain Technologien eher das Abrechnungsmodell zwischen Plattformen und Produzenten verändern werden, ist daher aktuell nicht absehbar.

Einige ausgewählte **Anwendungsfälle** für dezentrale Anwendungen in der **Kreativwirtschaft** sind:

Ujo Music ist ein Blockchain-basierter Prototyp für die Musikindustrie. Gemeinsam mit der britischen Künstlerin Imogen Heap wird hier an einer neuen, transparenteren und effizienteren Form der Musiklizenzierung gearbeitet.

Im Mai 2016 wurde im Rahmen des **Musictechfest** in Berlin das Thema Blockchain und Musikindustrie besprochen. Blockchain und die Musikindustrie waren auch ein großes Thema auf der **re:publica** 2016. Das Ziel: Transparenz von Urheberrechten und Abrechnungssystemen on the fly. Künstler bekommen ihren Anteil sobald konsumiert wird und nicht erst nach Monaten oder Jahren. Gelder werden direkt ausgeschüttet und müssen nicht erst durch Plattenlabels, Produzenten oder Vertriebsplattformen laufen. Über den Smart Contract erfolgen Konsum und Bezahlung zeitgleich und direkt.

Ascribe ist ein Dienst des Berliner Blockchain Startups BigchainDB. Künstler können ihre digitalen Kunstwerke oder Fotos ihrer analogen Kunstwerke für alle nachvollziehbar auf der Blockchain registrieren. Ein Hash Key (Digitales Zertifikat) wird generiert, mit dem der Urheber dieser Werke jederzeit seine Urheberschaft beweisen kann und auch die Rechte am Werk transferieren kann. Für die Zukunft sind Kooperationen mit online Marktplätzen angedacht. Hier soll es Künstlern ermöglicht werden, mit ihrem digitalen Zertifikat - ihrem Private Key - mit einem einfachen Mausklick die Rechte an ihren Kunstwerken auf online Marktplätzen temporär oder dauerhaft zu vermieten oder zu verkaufen.

2.4 Notare, Grundbücher und eGovernment

Zu den wichtigsten Anwendungsgebieten für Blockchain und Smart Contracts gehören jegliche Arten von Zertifizierungsstellen, Registrierungsstellen sowie notarielle Akte. Wenn eine Urkunde einmal auf der Blockchain registriert wurde, so ist diese digitale Urkunde für immer auf der öffentlichen Blockchain verschlüsselt verbrieft und kann von jedem eingesehen werden, der einen Autorisierungsschlüssel hat. Blockchain ist eine Technologie, mit der der Staat und staatsnahe Institutionen diese Prozesse besser und schlanker gestalten können.

Zertifizierungsstellen und Register wie zum Beispiel Ämter, die Grundstücksrechte verwalten, Eheschließungen dokumentieren, Patente gewähren und Ausweise ausstellen oder Anwälte, die Urheberrechte bestätigen, um nur einige zu nennen, können mit Blockchain-Technologie ersetzt oder effizienter gemacht werden und vermutlich auch ganz neue Leistungen anbieten. Bei Notaren, die Verträge verifizieren und Testamente besiegeln, besteht in Ländern wie Deutschland, in denen Grundbucheinträge und Register gut funktionieren, kein unmittelbarer Handlungsbedarf, da diese Prozesse weitgehend reibungslos und verlässlich funktionieren. Es gibt aber mittel- und langfristig erhebliche Einsparungspotenziale, da Transaktionen auf der Blockchain schneller, günstiger und weniger fehleranfällig sind. Länder in denen diese Dienste nicht gut funktionieren oder die korruptionsanfällig sind, werden tendenziell eher early adopter sein. Griechenland und Honduras beispielsweise wollen Grundbucheinträge und andere Verwaltungsakte in Zukunft auf die Blockchain umstellen. Aber auch Staaten, in denen das Grundbuchwesen reibungslos funktioniert, testen bereits die Blockchain. Schweden zum Beispiel befindet sich gerade in der Evaluierungsphase und testet Blockchain für Grundbucheinträge. Sony hat angekündigt, auf Blockchain-Basis ein Register auf den Weg zu bringen, das Studienfortschritte und die Echtheit von Bildungsabschlüssen überprüfbar macht.¹⁶

Steuerwesen: Die Blockchain hat das Potenzial, Buchhaltung und Steuerzahlungen zu revolutionieren. Dies ist kein unmittelbarer Anwendungsfall, sondern es bedarf noch erheblicher Netzwerkeffekte bevor er weitreichend umgesetzt werden könnte. Steuerzahlungen könnten langfristig viel effizienter durch Smart Contracts auf der Blockchain schon am Tag der Bezahlung von Rechnungen direkt vom Konsumenten an den Staat transferiert werden. Der mühsame, (semi)manuelle Erfassungsprozess durch Buchhaltungsabteilungen der betroffenen Firmen sowie deren Steuerberater, kann langfristig somit abge-

schaftt werden. Korruption und Steuerhinterziehung werden von vornherein vermieden. Steuern können on the fly - ohne Verzögerung - gezahlt werden. Diese Entwicklung bedarf allerdings einer weiten Verbreitung von Blockchain Technologien, der Einführung von Standards sowie von Maßnahmen regulatorischer Natur, die darauf abzielen, dass man buchhalterische und steuerliche Konsequenzen schon beim Buchen erkennt. Das deutsche Finanzamt ist zwar bei der digitalen Signatur schon dabei, Blockchain-basierte Steuerabwicklung einschließlich der Steuerprüfung on-the-fly ist aber vorerst eine eher theoretische Vision.

An dieser Stelle sei nochmals darauf hingewiesen, dass Blockchain-basierte Verfahren nicht notwendig den "gläsernen Bürger" erzwingen, sondern dass das erlaubte und erwünschte Level an Transparenz bei der Programmierung einer konkreten Anwendung festgelegt werden kann.

Genehmigungsverfahren: Am Beispiel von Baugenehmigungen oder Gewerbebeanmeldungen könnte man zeigen, wie man betroffene Prozesse einfacher über Smart Contracts auf der Blockchain abbilden kann. Lässt sich der Prozess des Erteilens einer Gewerbebeanmeldung beispielsweise über Standardisierung auf die Blockchain setzen? Können Behörden mittels spezieller Verifizierungscodes Kriterien überprüfen, und bei Erfüllung dieser Kriterien über den Smart Contract innerhalb weniger Stunden automatisch ein Gewerbe erteilen? All dies sind Anwendungsfälle, die es zu evaluieren gilt.

eGovernment: Abgesehen von den oben erwähnten Beispielen gibt es eine Vielzahl von Anwendungsfällen für Blockchain-basierte eGovernment Lösungen. Die Herausforderung wird möglicherweise darin liegen, das Potenzial dieser Technologien den beteiligten politischen Akteuren verständlich zu machen. Außerdem müssten alle Stakeholder, die an potenziellen Transformationsprozessen beteiligt sind, den politischen Willen zeigen; sonst sind Blockchain-basierte Projekte im eGovernment Bereich kaum durchsetzbar. Um sich an die Technologie heranzutasten, empfiehlt es sich daher, mit Pilotprojekten zu beginnen, um die Technologie und Anwendungsfälle in einem kontrollierten Rahmen zu verstehen, ohne sich gleich dazu zu verpflichten, jahrzehntelang etablierte Verwaltungsprozesse auf die Blockchain umzustellen. Pilotprojekte sind ein guter Proof of Concept, mit dem man Vertrauen schafft, um besser bewerten zu können, in welchem Bereich man auf die Blockchain umsteigen kann und will.

¹⁶ <http://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html>

2.5 Buchhaltung, Buchprüfung und Auditing

Traditionelle Buchhaltungs- und Buchführungsmethoden haben einheitliche Standards im Rechnungswesen geschaffen. Wenn man diese Standards mit Transaktionen auf der Blockchain verbindet, so kann man jegliche Finanztransaktion auf der Blockchain auch als zertifizierten Nachweis für Buchhaltung und Kostenrechnung verwenden. Ein Anwendungsgebiet der Blockchain ist daher die Buchhaltung.

Da Zahlungstransaktion auf der Blockchain gespeichert werden, kann man diese Transaktionen bei einheitlichen Buchführungsstandards auch gleich in ein Blockchain-basiertes doppeltes Buchhaltungssystem einführen. Somit gehören unabsichtliche Fehler in der Buchhaltung sowie aktive Verschleierung von Compliance-Verstößen der Vergangenheit an. Rechnungsprüfung besteht heute aus stichprobenhaften Buchprüfungen durch Innenrevisionen, Finanzämter und zertifizierte Buchprüfer. In Zukunft wird man diese Buchführungen durch Smart Contracts

auf der Blockchain automatisieren können. Privatsphäre ist hier allerdings ein Problem, mit dem man sich auseinandersetzen muss. Das erwünschte Niveau an Transparenz muss zwischen allen Beteiligten verhandelt und im Protokoll festgelegt werden.

Blockchain Technologien, ob private oder öffentliche Blockchains, ermöglichen Effizienzgewinne, auch für den Staat. Es würde sich unter anderem empfehlen, eine Forschungsgruppe aufzusetzen, die beispielsweise für den Anwendungsfall von Unternehmenssteuern durchkonjugiert, wie die Prozesse standardisiert werden müssten, um sie für alle Stakeholder zu optimieren. Dafür müssten dann Standards entwickelt werden, die auch international durchgesetzt werden müssten. Deutschland könnte hierbei eine Vorreiterrolle spielen, das Zeitfenster ist derzeit gegeben. Ein weiterer attraktiver Anwendungsfall könnte unter anderem die Prüfung der Verwendung öffentlicher Fördermittel sein.

2.6 Supply Chain

Blockchain-basierte Anwendungen können sich auf Vertriebsketten auf zweierlei Art auswirken: kürzere Vertriebswege und transparentere Vertriebsketten.

Kürzere Vertriebswege: Sobald genug Marktteilnehmer auf Blockchain-basierte Lösungen umgestiegen sind und einheitliche Daten und Transaktionsstandards entlang internationaler Vertriebsketten eingeführt sind, werden wahrscheinlich viele Marktteilnehmer irrelevant werden, die bislang zentrale Zertifizierungs- und Clearing Aufgaben übernommen haben. Allerdings nur dort, wo Makler, Großhändler oder Plattformen lediglich Clearing Funktionen innehaben. Jene Player, die einen zusätzlichen Mehrwert bieten, werden wahrscheinlich nicht so schnell ihre Rolle in der Supply Chain verlieren.

Transparentere Vertriebsketten: Ist Bio drinnen, wo Bio drauf steht? Ist Fair Trade drinnen, wo Fair Trade drauf steht? Ist 'Made in Germany' drinnen, wo 'Made in Germany' drauf steht?

Wo, wann und unter welchen Bedingungen wurden Einzelteile von Produkten und Dienstleistungen hergestellt? Was ist die genaue Herkunft von Produkten und Dienstleistungen? All diese Fragen können durch Blockchain Technologien transparenter und vertrauenswürdiger dargestellt und nachvollziehbar gemacht werden. Dies kann fundamentale Auswirkungen auf allgemeine volkswirtschaftliche Strukturen sowie konkrete betriebswirtschaftliche Aktivitäten haben. Das in Großbritannien beheimatete Startup provenance.org beschäftigt sich seit längerem mit diesen Fragen und entwickelt gerade einen Blockchain-basierten Prototyp. Zertifizierung und Qualitätssicherung auf der blockchain passiert 'on the fly' und bedarf in vielen Fällen keiner externen Organisationen mehr, die stichprobenartige ex-post Analysen machen. Ein weiterer Vorteil der Nachvollziehbarkeit von Vertriebsketten kann darin liegen, den betrügerischen Gebrauch gefälschter externer Zertifizierungen oder komplette Produktfälschungen deutlich zu erschweren.

2.7 Gesundheitswesen

Blockchain als Begriff ist auch im Gesundheitswesen angekommen und bereits auf dem Radar einiger Player. Allerdings befindet man sich im Wesentlichen noch in der Beobachtungs- und Evaluationsphase. Blockchain bietet auch im Gesundheitswesen ein großes Potenzial der Prozessoptimierung. Allerdings sind der medizinische Markt und das Gesundheitswesen stark reglementiert. Daher ist es wichtig zu verstehen, welche Anwendungsfälle technisch grundsätzlich möglich sind und welche Anwendungen Regularien unterworfen sind, die einen unmittelbaren Einsatz von Blockchain erschweren. Es sei denn, die Gesetzgebung zeigt hier den notwendigen politischen Willen, wie zum Beispiel im Fall von Estland, wo öffentliche Institutionen gemeinsam mit der Firma Guardtime alle Gesundheitsdaten in Estland auf die Blockchain migrieren¹⁷.

Zweiter Gesundheitsmarkt: In diesem Bereich sind die Teilnehmer in geringerem Maß gesetzlichen Regularien unterworfen. Es ist wahrscheinlich, dass wir hier die ersten Anwendungsfälle sehen werden. Datenkommunikation zwischen Arzt, Patient, weiteren Therapeuten und Krankenkassen könnte direkt über die Blockchain stattfinden. Kommunikation und Auswertung von Gesundheitsdaten sowie Frühwarnsysteme, sind ebenfalls naheliegende Anwendungen, beispielsweise überall dort, wo Patienten medizinisch-technische Endgeräte zur Verfügung

haben, mit denen sie regelmäßig ihre Werte messen: Diabetes, Blutdruck, Fitnesswerte. Der Patient erfasst Parameter über sein Endgerät und dann erfolgt automatisiertes Datenmonitoring ohne Zeitverzögerung und mit mehr Datensicherheit als durch herkömmliche Datenerfassungs- und Speicherungsverfahren. Dies ist insbesondere wertvoll für Frühwarnsysteme. Firmen wie Tierion¹⁸, Partner von Philips Blockchain Lab, arbeiten bereits an ähnlichen Lösungen.

Abrechnung zwischen Arzt, Patient und Krankenkassen:

Grundsätzlich kann die Bezahlung der niedergelassenen Ärzte, der Apotheken sowie das Abrechnungsverfahren der Krankenkassen durch Smart Contracts auf der Blockchain abgewickelt werden. Das könnte allen beteiligten Stakeholdern wesentlichen Zeit- und Kostenaufwand ersparen, sowie Abrechnungssysteme fehler- und manipulationsresistenter machen. Das Einsparungspotenzial bei den Transaktionskosten ist enorm. Dieser Anwendungsfall hängt jedoch einerseits von starken Netzwerkeffekten ab, andererseits auch von den beteiligten Interessengruppen und gesetzlichen Vorschriften, die in diesem Bereich erst angepasst werden müssten. Gem¹⁹ zum Beispiel ist ein US Amerikanisches Blockchain Startup, das in diesem Bereich die ersten use cases gemeinsam mit verschiedenen Stakeholdern im Gesundheitswesen testet.

¹⁷ <http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/>

¹⁸ <https://tierion.com/>

¹⁹ <https://gem.co/>

2.8 Energiewirtschaft

Transaktionseffizienz ist auch ein wichtiges Thema in der Energiebranche. Private Blockchain Lösungen und Konsortium Blockchains könnten ein guter Einstieg sein, um branchenweite Transaktionskosten zu senken. Vorreiter im Energiebereich in Deutschland ist unter anderem RWE. Ihr Ziel ist nicht nur, klassische Transaktionskosten zu senken, sondern auch komplett neue Geschäftsfelder zu erarbeiten, unter anderem auch auf Basis öffentlicher Blockchains wie Ethereum. Der RWE Innovation Hub beispielsweise beschäftigt sich mit neuen Geschäftsmodellen auf der Blockchain und hat hierzu mehrere Teams engagiert, die unter anderem auch in Berlin in interdisziplinären Projekten beschäftigt sind, nicht nur im klassischen Utility Bereich, sondern auch im sogenannten "Beyond Utility" Bereich. RWE versucht, Blockchain mit IoT und Physical Delivery zu kombinieren. Projektpartner in Berlin sind unter anderem Ethereum und der GTEC Innovationshub.

Peer to Peer Energy Trading: Die Energiewende in Deutschland will den Übergang von Kernenergie und nicht-nachhaltiger Nutzung fossiler Energieträger zu einer nachhaltigen Energieversorgung schaffen. Das hat dazu geführt, dass rund 50% der erneuerbaren Energien mittlerweile von genossenschaftlich strukturierten Kleinproduzenten produziert werden. Blockchain ist eine Technologie, mit der man solche genossenschaftlichen Strukturen einfach darstellen kann. Hier könnte die Kombination von Blockchain, IoT und Sharing Economy zum Tragen kommen, um die dezentrale Energieproduktion mit dezentraler Vertriebsstruktur zu koppeln. Die bisherige Herausforderung der Energiewende war weniger die erneuerbare Energie, sondern die Dezentralisierung des Stromhandels. Ein Großteil der Wertschöpfung im Energiehandel könnte mittels P2P-Energy Trading Systems vor Ort und regional stattfinden. Somit könnten wir in Deutschland eine weitere Phase der Energiewende erreichen.

Wo Blockchain neue Märkte eröffnet und alte Märkte ersetzt: Stromhandel ist in den meisten Ländern monopolisiert. Heutzutage kann man nur über einen Aggregator seinen selbst erzeugten Strom handeln. Alle Transaktionen laufen über die klassischen Energieanbieter. Dies ist eine wesentliche Markteintrittsbarriere für kleine Produzenten, die echten P2P-Handel verhindert, weil die Transaktionskosten durch administrative und regulatorische Hürden zu hoch sind. Auf der Blockchain wären erstmals Echtzeit-Märkte und Preisdifferenzierung möglich. Die größten Herausforderungen im Energiebereich sind nicht technischer Natur sondern regulatorischer Natur.²⁰ Der Strommarkt ist so reguliert, dass neue Marktteilnehmer und Startups oftmals an gesetzlichen Rahmenbedingungen scheitern. Ein Pilotprojekt auf regionaler Ebene könnte regulatorischer Skepsis entgegenwirken.

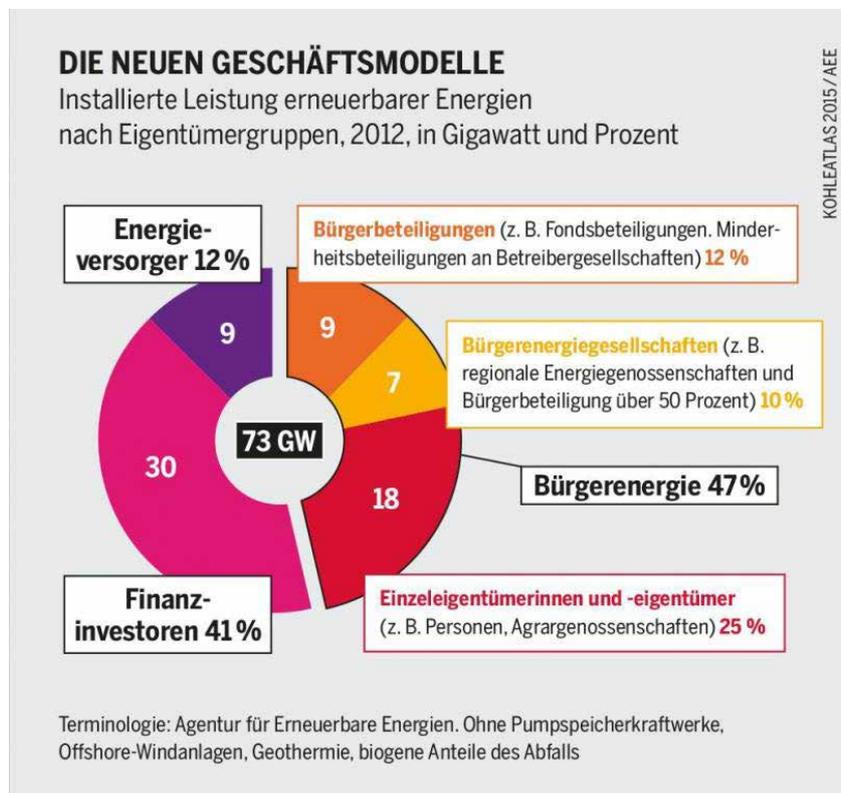
Solche Pilotprojekte ermöglichen staatlichen Akteuren einerseits, sich mit der Technologie in einem kontrollierten Rahmen vertraut zu machen. Sie helfen auch zu verstehen, welche gesetzlichen Rahmenbedingungen angepasst werden müssten, wenn man Blockchain-basierte Projekte im Energiebereich fördern will. Bisher sind bestenfalls für Mieterstrom-Modelle und Eigenverbrauch geklärt, welche Umlagen im Zuge der Energiewende (EEG-Umlage, Netzentgelte, u.v.m) an welcher Stelle fällig werden. Für den P2P-Energiehandel beispielsweise ist diese Frage bisher nicht geklärt.

Berlin könnte beispielsweise gemeinsam mit den Berliner Stadtwerken und entsprechenden Partnern in der Privatwirtschaft ein lokales "Smart Grid" Projekt für einen P2P-Energiehandel in einem kleinen kontrollierten Rahmen testen und evaluieren, ob Blockchain-basierte Lösungen auch in einem größeren Rahmen wirtschaftlich umsetzbar sind. Erste solche Pilotprojekte des Blockchain-basierten P2P-Energy Trading sind bekannt aus New York, wo im März 2016 der Betreiber LO3 Energy ein solches Netz mit je 5 produzierenden und konsumierenden Haushalten gestartet hat und aus Australien, wo das Unternehmen Power Ledger einen Feldversuch mit 20 Teilnehmern gestartet hat.

²⁰ Das Stromeinspeisegesetz (1990) und EEG Erneuerbare Energien Gesetz (seit 2000)

Abbildung 9

Die neuen Geschäftsmodelle in der Energiewirtschaft



Quelle: Kohleatlas 2015, Heinrich-Böll-Stiftung;
https://www.boell.de/sites/default/files/styles/fullsize/public/uploads/2015/05/energiewende_geschaeftsmodelle.jpg?itok=fs5aHCKt;
steht unter der Lizenz CC BY-SA 3.0 DE (<http://creativecommons.org/licenses/by-sa/3.0/de/legalcode>)

2.9 IT Dienstleistungen

Es gibt ein komplett neues Feld an Beratungsdienstleistungen im IT-Bereich rund um die Evaluierung und Implementierung von Blockchain-basierten IT-Lösungen und Geschäftsmodellen. BaaS, Blockchain as a Service, ist eines von vielen Schlagwörtern, wobei der Umfang der Leistungen hier variiert bzw. sich mit anderen Dienstleistungen vermischt. Etablierte Beratungsunternehmen und IT Dienstleister haben das Potenzial der Blockchain erkannt und bauen bereits Blockchain-basierte Lösungen auf. Microsoft (Azure)²¹, Deloitte (Rubix)²², IBM (BlueMix)²³, Amazon (AWS)²⁴ arbeiten bereits unter anderem daran, Blockchain as a Service (BaaS) über ihre Cloud Lösungen

anzubieten. Software Entwickler sollen dadurch in Zukunft single-click cloud-based Blockchain Lösungen bekommen, um rascher Blockchain-basierte Produkte entwickeln zu können. Die angedachten Lösungen basieren auf unterschiedlichen Blockchain Konzepten in Kombination mit Server-basierten Cloudlösungen. Aber es geht hier nicht nur um komplette BaaS Services sondern um einzelne Pilotprojekte. PricewaterhouseCoopers (PWC)²⁵ arbeitet unter anderem an einer Blockchain-basierten Lösung im Versicherungsgroßhandel für Echtzeit Auditing.

2.10 Legal Tech und neue juristische Sachverhalte

Die Schnittstelle zwischen Technologie und Privatrecht wird auf der Blockchain und im Dezentralen Web noch bedeutender als bisher. Smart Contracts beispielsweise sind keine Verträge klassischer Art in Form von Texten, die Vereinbarungen in Abschnitten und Paragraphen so darstellen, dass sie von Menschen, nämlich den Vertragsparteien und im Streitfall von einem Gericht interpretiert werden können, sondern Programme, die von Maschinen verstanden, kontrolliert (also auf das Eintreten der Bedingungen hin untersucht) und ausgeführt werden müssen. Allerdings haben sie praktisch die Wirkung von herkömmlichen Verträgen. Daher stellt sich unter anderem die Frage, wie man Smart Contracts rechtssicher und rechtskonform erstellen kann. Dies ist eine Frage, der Juristen in Zusammenarbeit mit Softwareentwicklern gemeinsam nachgehen müssen. Hier eröffnet sich ein großes Potenzial für Startups im Bereich Legal Tech.

Welches Recht gilt?

Eine viel grundlegendere Frage jedoch ist, welches nationale Recht in einem dezentralen P2P-Netzwerk, ohne Server, mit einer Vielzahl von international verteilten Netzwerkteilnehmern anwendbar ist. Nationale Rechtsformen und das komplizierte Geflecht von internationalen, bilateralen sowie multilateralen Verträgen werden schon lange nicht mehr den Anforderungen einer globalisierten Internet-basierten Gesellschaft gerecht. Im Dezentralen Web, wo die letzte zentrale Instanz, nämlich die des Servers, auch abgeschafft wird und Management durch Code ersetzt werden soll, wird die derzeitige Kluft zwischen nationalem Recht und der Realität des Internets noch größer als zuvor. Öffentliche Blockchains wie Bitcoin und Ethereum sind per se dezentral. Die darauf bauenden dApps können auch in die Kategorie fallen, und DAOs sind es schon per Definition. Welches Recht gilt also, wenn ein Unternehmen dezentral organisiert ist und keinen klassischen Firmensitz hat? Welche gesellschaftsrechtliche Form ist in so einem Fall sinnvoll und anwendbar? Auch steuerrechtliche Aspekte, Gewährleistungs- und Haftungsverpflichtungen u.v.m sind derzeit kaum geklärt.

²¹ <https://azure.microsoft.com/en-us/solutions/blockchain/>

²² <http://rubixbydeloitte.com/>

²³ <http://www.wsj.com/articles/ibm-bets-on-bitcoin-ledger-1455598864?mg=id-wsj>

²⁴ <http://www.the-blockchain.com/2016/05/03/amazon-announced-blockchain-service-baas-sandbox-developers/>

²⁵ <http://www.coindesk.com/pwc-blockchain-project-creates-living-audit-wholesale-insurance/>

Tokensales von Blockchains, dApps und DAOs

Im Gesellschaftsrecht gibt es keine adäquaten Lösungen für dezentrale Organisationen. Es gibt derzeit keine Gesellschaftsform, die den Anforderungen einer dezentralen Organisation mit international verteilten Netzwerkteilnehmern wirklich gerecht wird. Deswegen wählen viele Blockchain, dApps und DAO Projekte derzeit den Umweg von komplexen Rechtskonstrukten in der Schweiz. Die Frage der Gesellschaftsform und der damit verbundenen Haftungsbeschränkungen ist vor allem im Zusammenhang mit Blockchain, dApp und DAO Tokensales wichtig, um den Gründern und Netzwerkteilnehmern mehr Rechtssicherheit zu geben. Es herrscht derzeit große Unklarheit über den Rechtsstatus solcher Tokensales. Viele Blockchains, dApps und DAOs finanzieren sich durch sogenannte Tokensales. Dabei veräußert der Betreiber bzw. Entwickler der dApps eigene dApp-spezifische Tokens²⁶, die weiterverkauft werden können. Zusätzlich zu den öffentlichen Blockchain-Tokens (Bitcoin, BTC bei der Bitcoin Blockchain,

Ether, ETH bei der Ethereum Blockchain, u.v.m), gibt es dApp-Tokens (REP bei Augur, SNGLS bei SingularDTV, u.v.m), und DAO Tokens (DAO bei The DAO²⁷ u.v.m). In manchen Fällen sind diese Tokens keine Anteile, sondern die netzwerkeigene Währung. In anderen Fällen sind sie ein wichtiger Bestandteil des spieltheoretischen Anreizmechanismus. Die Grenzen verschwimmen hier oftmals, zumal auf der Blockchain komplett neue Marktmechanismen und wirtschaftliche Dynamiken eintreten, die von manchen als Crypto Economics bezeichnet werden und für die es noch keine Rechtsrahmen gibt.

Wie Rechtssicherheit durch anwaltliche Tätigkeit sichergestellt werden kann, ist in der Praxis kaum erprobt. Es liegt auch noch kaum Rechtsprechung vor. Mehr Rechtssicherheit in solchen Fragen würde mehr Sicherheit für Unternehmensgründer, Entwickler, Anwender und Anteilseigentümer an solchen Konstrukten schaffen. Eine vorbeugende Überregulierung ist allerdings zu vermeiden, um Innovation nicht im Keim zu ersticken.

2.11 Forschungsbedarf

Obwohl Blockchain-Technologien längst der Grundlagenforschung entwachsen sind, gibt es dennoch in der angewandten Forschung erheblichen Forschungsbedarf, der sowohl durch Unternehmen als auch durch angewandte Forschung im öffentlichen Sektor bearbeitbar ist. Eine Auswahl solcher Forschungsbereiche ist: Skalierung von Blockchains, Identity Lösungen sowie Anonymität, IT Sicherheit, juristische Herausforderungen von dezentralen Rechnersystemen, neue

ökonomische Modelle, Geschäftsprozessmodellierung und viele weitere Themen. "Es ist davon auszugehen, dass wir in ein bis zwei Jahrzehnten wirtschaftlich über Mechanismen miteinander interagieren werden, für die wir bislang weder Konzepte noch Begriffe haben."²⁸ Die nächsten Jahre werden daher voraussichtlich noch viele neue Forschungsfelder zu Tage bringen, von denen wir heute noch keine Vorstellung haben.

²⁶ Token, wörtlich: Zeichen, Gutschein, Wertmarke, Jeton

²⁷ The DAO (<http://daohub.org>) war eine spezielle Ausprägung einer DAO, und mitunter eines der ersten Experimente mit dem Konzept von Dezentral Autonomen Organisationen. The DAO ist im Sommer 2016 in die Schlagzeilen geraten. Erst, weil es in einem spektakulären Tokensale innerhalb von 4 Wochen rund 180 Millionen EUR im Gegenwert von Ether auf die Beine gestellt hat, dann als rund 50 Millionen EUR temporär "gedrained" wurden. Letztendlich wurde eine Lösung gefunden, und die Tokens sind an die ursprünglichen Tokenholder zurückgeflossen. Die Details der Ereignisse würden den Rahmen dieser Arbeit sprengen. Eines aber ist hier wichtig anzumerken: All diese Ereignisse haben viele wichtige Fragen rund um Smart Contract Security und Governance Mechanismen von dezentralen Organisationen aufgeworfen. Hier besteht viel Handlungsbedarf im Bereich FuE.

²⁸ Bitcoin Kurz & Gut, Jörg Platzer, 2014, Seite 92 (Kindle Version)

3. Standort Berlin

Berlin ist weltweit nach London und New York einer der Hauptknotenpunkte für Blockchain Entwickler. Der Grund hierfür liegt einerseits darin, dass Berlin eine blühende Kreativ- und Startup Szene hat. Andererseits hat Berlin in der Vergangenheit international namhafte Entwickler aus der Kryptografie- und Bitcoin Szene angezogen. Einer der Gründe hierfür ist, dass Deutschland in seiner Gesetzgebung bisher einen hohen Wert auf Anonymität und Privatsphäre gelegt hat.

Viele wesentliche Blockchain Basistechnologien werden von Berliner Startups entwickelt (Ethereum, Ethcore, BigchainDB, IPDB, viele Bitcoin Wallet Entwickler, u.v.m). Einige dieser Firmen haben zwar ihren offiziellen Firmensitz in anderen Ländern, wie Großbritannien und den Niederlanden, allerdings sitzt ein großer Teil ihrer Entwicklerteams in Berliner Büros. Der Nährboden für spannende Blockchain-basierte Projekte sowie der potenzielle Zulauf von Investitionskapital, Talenten und Arbeitsplätzen ist daher als groß einzuschätzen.

3.1 Startups

In Berlin gibt es eine blühende Szene von jungen, motivierten Unternehmen, Softwareentwicklern, kreativen Köpfen und zunehmend mehr Investoren, die bereit sind, am Standort zu

investieren. Berlin hat die Chance, sich als einer der Blockchain Hotspots weltweit zu etablieren und mehr talentierte, qualifizierte und motivierte Arbeitskräfte anzuziehen.

Dies ist eine exemplarische Auflistung von Berliner Blockchain Startups und Playern (Kein Anspruch auf Vollständigkeit):

- **All4btc**, FinTech, Bezahl Dienstleistung
- **Bitwala**, FinTech, Bezahl Dienstleistungen (Teil des Teams in Berlin)
- **Bitbond**, FinTech, Darlehen
- **Blockchain Industries**, Basistechnologie
- **BigchainDB**, Basistechnologie, Datenbank
- **BlockchainHub**, InformationsHub und Think Tank
- **Blueyard Capital**, Venture Capital Firma, auf Blockchain Projekte spezialisiert
- **Coynoare**, FinTech, Beratung
- **Electrum Technologies GmbH**, FinTech, Basistechnologie, Bitcoin Wallet
- **Ethdev**, das Berliner Entwicklerteam von ethereum.org, Basistechnologie
- **Parity**, Basistechnologie
- **Monax**, Basistechnologie
- **IOTA**, Basistechnologie, IoT
- **IPDB**, Interplanetary Database, Basistechnologie
- **Jolocom**, Basistechnologie
- **Leondrino**, FinTech (Teil des Teams in Berlin)
- **Lisk**, Basistechnologie, (Teil des Teams in Berlin)
- **Slock.it**, Basistechnologie, IoT, (Teil des Teams in Berlin)
- **SatoshiPay**, FinTech, Nanopayment Service
- **Vaultoro**, FinTech, Börse

3.2 Etablierte Firmen und Institutionen im Blockchain Umfeld

Bestehende Firmen, ob Großkonzerne oder etablierte Startups, sind bis auf wenige Ausnahmen größtenteils noch nicht aktiv. Immer mehr Unternehmen haben zwar Blockchain als Technologie bereits entdeckt, befinden sich allerdings noch in der Beobachtungsphase. Diesen Firmen scheint es aktuell vor allem wichtig zu sein, die Technologie dahinter und das Potenzial der Anwendungen überhaupt erst zu verstehen und zu evaluieren,

wie Blockchain die eigene Branche und die eigenen Geschäftsfelder betreffen könnte. Manche größeren Unternehmen sind dabei, in-house Think Tanks oder Innovationshubs aufzusetzen, die sich zum Teil und manchmal auch ausschließlich dem Thema widmen. Einige führen ihre Aktivitäten, wie oben am Beispiel RWE gezeigt, auch in Berlin durch.

3.3 Forschung und Lehre

Einzelne Institute unterschiedlicher Universitäten und Fachrichtungen in Berlin beschäftigen sich bereits mit Blockchain-Technologien, sowohl in der Forschung als auch in der Lehre, unter anderem: Prof. Björn Scheuermann, HU Berlin, Institut für Informatik (Geldwertstabilität und die Schnittstelle von Technik und Mikroökonomie), Prof. Stefan Tai, TU Berlin, Institut Wirtschaftsinformatik und quantitative Methoden (Skalierung und Anwendungsarchitekturen von Blockchains, Verteilte Systeme), Prof. Ute Dietrich, HTW, Wirtschaftsingenieurwesen mit dem Schwerpunkt Informatik (IoT und Industrie 4.0), Prof. Katha-

rina Adam, HTW, Allgemeine BWL (Corporate Finance, Blockchain, Investition Finanzierung und Rechnungswesen), Prof. Peter Hufnagel, HTW, Angewandte Informatik, Gesundheitsinformatik, Telemedizin, Medical Imaging (Telemedizinetechnik, Blockchain, Gesundheitsökonomie), Christoph Burger, ESMT, Associate Dean of Executive Education (dezentrale Energiemärkte), Prof. Manfred Hauswirth, TU Berlin (Fachgebiet Verteilte offene Systeme sowie Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS), Badi Farzaneh, Phd Candidate, HIIG (Internet Governance, Blockchain Governance).

3.4 Meetups in Berlin

- Bitcoin Stammtisch im Room77
- BlockchainMeetup Berlin
- BlockchainHub Meetup
- Ethereum Meetup

4. Potenziale und Herausforderungen

Derzeit scheint die Finanzindustrie im Blockchain Bereich die Nase vorn zu haben. Aber die anderen Branchen ziehen bereits nach. Das größte Potenzial von Blockchain ist Transaktionseffizienz und Dezentralisierung. Die größte Herausforderung scheint im Moment darin zu liegen, Wissen und Verständnis dazu zu verbreiten, was Blockchain, dApps und Smart Contracts sind und was man damit konkret machen kann. Auch ist in vielen Fällen nicht klar, wie man überhaupt

mit dApps auf Public Blockchains Geld verdienen kann, wenn der Code open source ist. Das ist allerdings nur ein Zeichen dafür, dass die Technologie noch sehr jung ist. Genauso wie bis Ende der 1990er Jahre die meisten nicht abschätzen konnten, bzw. skeptisch waren, ob und wie man mit Online-Content Geld verdienen kann und es Mitte der 2000er Jahre schwierig abzusehen war, wie sich mobile Apps monetarisieren lassen.

Abbildung 10

Potenziale und Herausforderungen

Potenziale	Herausforderungen
Effizienz P2P Transaktionen durch Dezentrale Transaktionsvalidierung	Skalierbarkeit Transaktionen pro Sekunde; Webstacks und Libraries, um schneller programmieren zu können
Nachvollziehbarkeit Erhöhte Fälschungssicherheit und Nachvollziehbarkeit von Produktions- und Zahlungsketten	Usability Handling von public private key und user interfaces
Transparenz Erhöhte Nachvollziehbarkeit, Transparenz und daher weniger Willkür	Geschäftsmodelle Wie kann man mit dApps in Zukunft Geld verdienen, wenn der Code open source ist?
	Abhängigkeit von komplexen Algorithmen Sind Smart Contract und komplexe Algorithmen der neue „Man in the Middle“?
	Reputation Systems Im dezentralen Web braucht man gute Reputation Systems, um Entscheidungen auch dezentralisieren zu können.

Quelle: eigene Darstellung

Blockchain und das Dezentrale Internet können in jedem Fall Game Changer sein. Aber je nach Branche wird die Technologie in manchen Fällen früher, in anderen Fällen später relevant werden, vor allem überall dort, wo Netzwerkeffekte notwendig sind. An einigen Aspekten der Protokolle und Anwendungen besteht noch Forschungs- und Entwicklungsbedarf:

Skalierbarkeit (Anzahl der Transaktion pro Sekunde), Private Key Management sowie benutzerfreundliche Interfaces sind weitere Herausforderungen. Die Frage, die sich hier stellt, ist nicht, ob diese Probleme gelöst werden können, sondern eher wann und wie genau sie gelöst werden.

Timing ist daher eine der wichtigsten Fragen. Es könnte durchaus sein, dass das "Tal der Tränen" nahe ist. Wie wir in der Vergangenheit gesehen haben, gibt es bei den meisten

Technologien einen Hype Cycle: die Erwartungshaltung ist hoch, viel Geld wird in eine Industrie/Technologie gepumpt, dann werden manche Investoren nervös. Vor allem jene, die nur auf kurzfristige Gewinne aus sind oder die Technologie nicht wirklich verstehen. Wenn es den meisten Investoren nicht schnell genug geht, kommt es in weiterer Folge zum Einbruch der Investitionen. Das bedeutet allerdings nicht, dass eine Technologie, besonders nach Einsetzen der Netzwerkeffekte, nicht das Potenzial hat, das erwartet werden durfte, sondern spricht eher dafür, dass manche Akteure die notwendigen Zeitfenster falsch einschätzen. Es ist daher anzunehmen, dass so ein Zyklus auch bei Blockchain eintreten wird. Jene, die es schaffen, diese Phase durchzuhalten, werden wahrscheinlich erfolgreich sein.

5. Handlungsempfehlungen für den Standort Berlin

Blockchain hat das Potenzial, eine völlig neue Art der Abwicklung von Geschäften zu ermöglichen und zum neuen Geschäftsfeld innerhalb der IT zu werden. Blockchain hat damit auch das Potenzial, einen dauerhaften umfassenden digitalen Wandel von Wirtschaft und Gesellschaft mit sich zu bringen oder diesen mindestens zu beschleunigen. Daher ist es nicht nur wichtig, unmittelbare wirtschaftliche Handlungsfelder zu beleuchten, sondern das Thema auch langfristig und interdisziplinär zu betrachten mit dem Fokus, neue wirtschaftliche und gesellschaftliche Lösungen auf Basis dezentraler Blockchain Technologien zu entwickeln.

Obwohl Blockchain eine noch junge Technologie ist, sind viele Potenziale heute schon greifbar, vor allem im Finanzsektor. Viele weitere Anwendungen sind bereits in Entwicklung. In einer breiten Masse gibt es allerdings noch viel zu wenig Information und Wissen über diese Technologie, sowohl bei Entwicklern und IT-Anbietern, als auch bei potenziellen Anwendern. Jetzt kommt es darauf an, das Thema Blockchain in die Öffentlichkeit zu bringen, wenn man als Standort profitieren will. Mögliche Unterstützungsmaßnahmen sollten deshalb - wie bei jeder neuen Technologie - darauf zielen, Rahmenbedingungen zu schaffen, die Neugierde und Experimentierfreudigkeit fördern, anstatt einem Mindset von "das haben wir noch nie so gemacht" nachzugeben.

5.1 Förderungen von Pilotprojekten

Etablierte Unternehmen, auch die öffentliche Verwaltung, sollten angeregt werden, neue Blockchain-basierte Technologien in Test- und Pilotprojekte zu adoptieren. Die Berliner Verwaltung könnte gemeinsam mit privaten Unternehmen erste eGovernment Lösungen im Rahmen solcher Pilotprojekte testen. Privatwirtschaftliche Akteure könnten in unterschiedlichen Branchen mit Unterstützung des Landes Pilotprojekte

starten, um in einem kontrollierten Rahmen die Technologie besser zu verstehen. Für Pilotprojekte bieten sich folgende im jeweiligen Kapitel genauer ausgeführte Themen an: Erneuerbare Energien (P2P-Stromhandel am Beispiel des TransActive Grid in New York), Grundbucheinträge, jegliche Art von Genehmigungsverfahren, Medizindaten und Supply Chain.

5.2 Rechtssicherheit schaffen

Für Blockchains, dApps und DAOs ist derzeit unklar, in wie weit sich der Rechtsrahmen des nationalen Rechts (Gesellschaftsrecht, Steuerrecht, Arbeitsrecht, Konsumentenrecht, u.v.m) auf dezentrale Konstrukte übertragen lässt. Hier sollte auch auf lokaler sowie nationaler Ebene geprüft werden, ob ein Regulierungsbedarf besteht und gegebenenfalls ein entsprechender Rechtsrahmen geschaffen werden, der solche Innovationen rechtssicher ermöglicht, ohne Innovation zu erschweren. Der lokale Handlungsspielraum ist allerdings beschränkt, da diese Fragen langfristig weder auf lokaler noch auf nationaler Ebene zufriedenstellend gelöst werden

können und es in vielen Fällen konsistenter, internationaler Lösungen Bedarf. Deutschland könnte aber beim Setzen solcher internationalen Standards eine Vorreiterrolle spielen. Des Weiteren kann man lokale Initiativen starten, die Rechtsspraktiker mit Blockchain-Themen vertrauter machen. Der Berliner Blockchainhub beispielsweise hat gemeinsam mit der Berliner Zweigstelle der internationalen Anwaltskanzlei DLA Piper und namhaften Entwicklern aus dem Blockchain Umfeld einen Arbeitskreis zum Thema Blockchain & the Future of Law etabliert, wo man sich genau damit auseinandersetzt.

5.3 Information und Ausbildung

Informationsaufarbeitung: Es gibt nach wie vor zu wenig Information über die Blockchain, vor allem deutschsprachige Information, die auch einem technisch nicht versierten Publikum verständlich ist. Einen ersten Schritt in Richtung der interessierten Fachöffentlichkeit stellt dieser Report dar. Das Thema Blockchain sollte allerdings für eine breitere Öffentlichkeit aufgearbeitet, kommuniziert und interdisziplinär propagiert werden. Die Anwendungsthemen in einer Vielzahl von Branchen sind im Kapitel 3 benannt. Besonderer interdisziplinärer Aufarbeitung bedürfen insbesondere die Aspekte an der Schnittstelle zwischen Technologie und Recht oder Verwaltung (Smarts Contracts und das Rechtssystem, eGovernment, volkswirtschaftliche Auswirkungen von Blockchain).

Bildung: Um Berlin als Wirtschaftsstandort zu stärken, wird es wichtig sein, bestehende und zukünftige Arbeitnehmer und Unternehmensgründer mit den notwendigen Fähigkeiten auszustatten. Notwendige Kenntnisse über Systemarchitektur und Programmierung müssen nun in der Ausbildung ankommen und sollten an Fachhochschulen, Universitäten und arbeitsmarktnahen Bildungseinrichtungen angeboten werden. Dafür müssen so schnell als möglich gemeinsam mit den Stakeholdern Blockchain relevante Lehrpläne und Unterrichtsmaterialien entwickelt werden.

5.4 Kooperationsnetzwerke und Veranstaltungen

Mit dem Ziel, eine Plattform für Ideen und neue Lösungen rund um Blockchain zu schaffen, sollten Events und Kooperationsnetzwerke eingerichtet bzw. gefördert werden, die Informationen rund um Blockchain aufarbeiten, den unter-

schiedlichen Akteuren in Berlin vermitteln und diese Akteure auch bei regelmäßigen Veranstaltungen verschiedener Formate zusammenbringen: Firmen, Bildungs- und Forschungseinrichtungen sowie Privatpersonen.

Abbildung 11

Bereichsübergreifende Netzwerke

Bereichsübergreifende Netzwerke
HR-Entwicklung, Bildung und Lehre
Forschung und Entwicklung
KMUs und Unternehmensgründer
Engagierte Privatpersonen

Quelle: eigene Darstellung

5.5 Förderung von Basistechnologien und Blockchain Startups

Es gibt eine Reihe von Maßnahmen, die darauf abzielen könnten, den Standort Berlin mit gezielter Förderung von Blockchain-basierten Aktivitäten und Projekten zu fördern.

Kooperation von Wirtschaft und Universitäten: Es würde sich anbieten, niedrighschwellige Förderungen einzuführen, die die Annäherung von Unternehmen unterschiedlicher Branchen und Unternehmensgrößen an das Thema unterstützen. Dazu könnte sowohl die Nutzung des Transferbonus für diesen Zweck stärker beworben werden als auch die Nutzung von Blockchain-Technologien explizit als möglicher Gegenstand von Coachings im Rahmen des Coaching Bonus gefördert werden. Viele Unternehmen scheinen die beiden Programme im Zusammenhang mit Blockchain bisher nicht wahrzunehmen. Darüber hinaus erscheint die Einrichtung einer blockchain-

spezifischen Beratungs- oder Transferstelle über einen Zeitraum von drei Jahren im Umfang einer vollen Stelle an einer Hochschule sinnvoll.

Forschung und Entwicklung: Bei der technischen Forschung gibt es Herausforderungen im Bereich Skalierbarkeit von Blockchains, Netzwerksicherheit von P2P-Netzen, Smart Contract Security sowie Datensicherheit und Privacy. Interdisziplinärer Forschungsbedarf besteht bei Fragen rund um Geschäftsmodelle, Soziologie, Volkswirtschaft, Politik und Recht, Rechnungswesen und Unternehmenssteuern. Derzeit sind insbesondere die juristischen Fragen, sowie Fragen rund um Governance dezentraler Organisationen wichtig. Hier sollte entsprechende FuE ebenso gefördert werden wie die gezielte Entwicklung interdisziplinärer FuE-Projekte.

Abbildung 12

Bereichsübergreifende Forschung zu Blockchain-Themen

Bereichsübergreifende Forschung zu Blockchain-Themen
Politikwissenschaft
Volkswirtschaft
Soziologie
Neue Geschäftsmodelle
Recht
Informatik
Kryptografie

Quelle: eigene Darstellung

Interviewpartner

Adam, Katarina: Prof. Dr. Ing. (HTW, Hochschule für TEchnik und WIRtschaft)
Badiei, Farzaneh: Phd Candidate, (HIIG, Humboldt Institut für Internet und Gesellschaft)
Borchers, Peter: MBA, (Geschäftsführer, Allianz X)
Burger, Christoph: MBA, (ESMT, European School of Management and Technology)
Crane, Brian-Fabian: Msc, (Monax und Organisator des Blockchain Meetups Berlin)
Hasberg, Kirsten: MSc (Energy Democracy)
Hauswirth, Manfred: Prof. Dr. (Fraunhofer Fokus)
Hufnagel, Peter: Prof. (Charite und HTW)
Lohkamp, Joachim: MBA (Gründer und Geschäftsführer Jolocom)
McConaghy, Masha: PhD (CCO of BigchainDB/Ascribe)
McConaghy, Trent: PhD (CTO BigchainDB/IPDB)
Ciarán, O'Leary: Dipl. Kfm, (Geschäftsführer, Blueyard Capital)
Remmers, Karl-Heinz: Dipl. Ing. (Vorstand Solarpraxis Neue Energiewelt AG)
Scheuermann, Björn: Prof. Dr. (Humboldt Universität Berlin)
Stöcker, Carsten: Dr. Dipl. Phys. (RWE Innovation Lab, Innovations Manager)
Susemihl, Ingo: Dipl. Ing. (Siemens Novel Business, Venture Manager)
Wattendrupp, Claus: (Vattenfall, Leiter Business Development Erneuerbare Energien)

Quellen und weiterführende Informationen

Diese Studie beschreibt den aktuellen Stand der Entwicklung zum Zeitpunkt der Herausgabe dieser Studie. Blockchain und alle anderen Technologien rund um das Dezentrale Web sowie deren Anwendungen sind einem rasanten Wandel unterworfen. Obwohl darauf geachtet wurde diese Studie so neutral und vorausschauend wie möglich zu verfassen, können einige Fakten bereits kurze Zeit nach Erscheinen dieser Studie nicht mehr aktuell sein. Die wenigen Bücher, die es zu dem Thema gibt, sind derselben Problematik unterworfen. Aktuellere Informationen bieten meist einschlägige, im Folgenden angeführte online Medien, die allerdings oft ebenfalls mit der rasanten Entwicklung nicht Schritt halten. Gerade bei öffentlichen Blockchains ist die aktuellste Information zum Stand der öffentlichen

Diskussion den sozialen Netzwerken zu entnehmen, was dem open source Charakter von öffentlichen Blockchains geschuldet ist.

Quellen zum Thema Blockchain, insbesondere zu aktuellen Aktivitäten von Unternehmen oder Institutionen, sind fast durchweg Internet-Quellen, deren Links sich rapide ändern. Auf die Angabe solcher Fundstellen wurde deshalb weitgehend zu Gunsten eines Verzeichnisses weiterführender Literatur verzichtet. Informationen dieser Art stammen oftmals aus Pressemeldungen und Unternehmensmeldungen, die zum Zeitpunkt der Recherche online waren. Viele weitere Informationen entstammen der beruflichen Tätigkeit der Autorin und einzelnen Fachinterviews, für die an dieser Stelle nochmals gedankt sei.

Bücher

- Bitcoin - Kurz und Gut, Jörg Platzer, 2014
- Blockchain Revolution, Don Tapscott, 2016
- The Business Blockchain, William Mougayar, 2016

Weiterführenden Online Ressourcen

- Allgemeine Infos, Blockchain für Einsteiger: <http://blockchainhub.net>
- ÖFIT-Trendschau, 2016, Fraunhofer institut FOKUS, Jens Fromm und Mike Weber, <http://www.oeffentliche-it.de/-/blockchain>
- Bitcoin: <https://bitcoin.org/>
- Ethereum: <https://blog.ethereum.org/>
- IPFS: <https://ipfs.io/>
- IPDB: <https://ipdb.foundation/>
- Bitcoin White Paper: <https://bitcoin.org/bitcoin.pdf>
- Ethereum White Paper: <https://github.com/ethereum/wiki/wiki/White-Paper>
- BigchainDB White Paper: <https://www.bigchaindb.com/whitepaper/>
- Web3: <http://gavwood.com/web3lt.html>
- <http://www.coindesk.com/blockchains-and-the-future-of-audit/>
- <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>
- <http://www.economist.com/news/special-report/21650295-or-it-next-big-thing>
- <https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services>
- <https://www.weforum.org/agenda/2015/12/how-blockchain-technology-could-change-the-world>

Online Nachrichtenportale und Blockchain relevante Blogs

- <http://www.coindesk.com/>
- <https://cointelegraph.com/>
- <https://bitcoinmagazine.com/>
- <https://www.cryptocoinsnews.com/>
- <https://letstalkbitcoin.com/>

Die Technologiestiftung Berlin engagiert sich für die Entwicklung Berlins zur Hauptstadt der Digitalisierung. Sie macht die Chancen und Perspektiven deutlich, die mit dem technologischen Fortschritt verbunden sind und formuliert Handlungsempfehlungen. Außerdem unterstützt sie die Open Data-Strategie und setzt sich für eine smarte Infrastruktur ein.

Dr. Shermin Voshmgir

Dr. Shermin Voshmgir ist Gründerin des BlockchainHubs, einem Informations-Hub und Think Tank mit Sitz in Berlin, der weltweit interdisziplinär die Entwicklung der Blockchain-Technologie vorantreibt, kommuniziert und diskutiert. Sie ist studierte und promovierte Wirtschaftsinformatikerin. Aktuell lehrt sie als Gastdozentin zum Thema Blockchain am Institut für Informatik der Wirtschaftsuniversität Wien und ist eine gefragte Vortragende bei Konferenzen zum Thema Blockchains, Smart Contracts und dem dezentralen Web. Zudem berät sie in diesem Zusammenhang Unternehmen zu relevanten Blockchain-Anwendungen und Regierungsorganisationen bezüglich notwendiger Neugestaltung der Gesetzgebung.